P-2301R/RL-P1C

VoIP Station Gateway

(With Lifeline)

Support Notes

Version 3.60

March 2007

ZyXEL

Unleash Networking Power

INDEX

Application Notes 5
General Application Notes 5
Internet Connection 5
Setup the ZyXEL device as a DHCP Relay 10
Configure an Internal Server Behind SUA 12
Configure a PPTP server Behind SUA 14
About Filter & Filter Examples 18
Using the Dynamic DNS (DDNS) 42
Network Management Using SNMP 43
Using syslog 50
Using IP Alias 53
Using IP Multicast 57
Using Prestige traffic redirect 59
Using Universal Plug n Play (UPnP) 62
VoIP Application Notes 69
Setup SIP Account 69
Phone port settings 74
Phone book Speed dial 76
FAQ 78
ZyNOS FAQ 78
What is ZyNOS? 78
How do I access the embedded web configurator? 78
What is the default LAN IP address and Password? Moreover, how do I change it? 79
How do I upload the ZyNOS firmware code via embedded web configurator? 79
How do I upgrade/backup the ZyNOS firmware by using FTP client program via LAN? 79
How do I upload or backup ROMFILE via web configurator? 80
How do I backup/restore configurations by using FTP client program via LAN? 80
Why can't I make Telnet to Prestige from WAN? 80
What should I do if I forget the system password? 81
What is SUA? When should I use SUA? 81

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

What is the difference between NAT and SUA? 81
How many network users can the SUA/NAT support? 82
What are Device filters and Protocol filters? 82
Why can't I configure device filters or protocol filters? 82
Product FAQ 82
Is the ZyXEL device an Internet Access Sharing Router? 82
Will the ZyXEL device work with my Internet connection? 83
What do I need to use the ZyXEL device? 83
What is PPPoE? 83
Does the ZyXEL device support PPPoE? 83
How do I know I am using PPPoE? 84
Why does my provider use PPPoE? 84
Which Internet Applications can I use with the ZyXEL device? 84
How can I configure the ZyXEL device? 84
What network interface does the ZyXEL device support? 84
What can we do with Prestige? 84
Does Prestige support dynamic IP addressing? 84
What is the difference between the internal IP and the real IP from my ISP? 85
How does e-mail work through the ZyXEL device? 85
What is the difference between the 'Standard' and 'RoadRunner' service? ..85
Is it possible to access a server running behind SUA from the outside Internet? If possible, how? 86
What DHCP capability does the ZyXEL device support? 86
How do I used the reset button, more over what field of parameter will be reset by reset button? 86
What network interface does the new Prestige series support? 86
How does the ZyXEL device support TFTP? 86
Can the ZyXEL device support TFTP over WAN? 86
How can I upload data to outside Internet over the one-way cable? 87
How fast can the data go? 87
My Prestige can not get an IP address from the ISP to connect to the Internet, what can I do? 87
What is BOOTP/DHCP? 90
What is DDNS? 90
When do I need DDNS service? 91

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

What DDNS servers does the ZyXEL device support? 91
What is DDNS wildcard?....91
Does the ZyXEL device support DDNS wildcard? 91
Can the ZyXEL device SUA handle IPsec packets sent by the VPN gateway behind Prestige?....91
How do I setup my Prestige for routing IPsec packets over SUA? 92
VoIP FAQ 92
What is Voice over IP? 92
How does Voice over IP work? 92
Why use VoIP? 92
What is the relationship between codec and VoIP?....93
What advantage does Voice over IP can provide?....93
What is the difference between H.323 and SIP?....93
Can H.323 and SIP interoperate with one another?....93
What is voice quality?....93
How are voice quality normally rated?....93
What is codec? 94
What is the relation of codec and VoIP? 94
What codec does Prestige support?....94
Which codec should I choose?....94
What do I need in order to use SIP? 94
Unable to register with the SIP server?....95
I can register but can not establish a call?....95
I can make a call but the voice only goes one way not bothway? 95
I can receive a call but the voice only goes one way not bothway? 95
If all the about have been tried, but register still fail what should I do?....95
I suspect there is a hardware problem with my Prestige what should I do? 96
Trouble Shooting 96
Unable to Get WAN IP from ISP 96
Using Embedded Packet Trace 100
Debug PPPoE Connection 115
CLI Command List....126

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

Application Notes

General Application Notes

Internet Connection

A typical Internet access application of the ZyXEL device is shown below. For a small office, there are some components needs to be checked before accessing the Internet.

- Before you begin
- Setting up the Windows
- Setting up the ZyXEL device router
- Troubleshooting

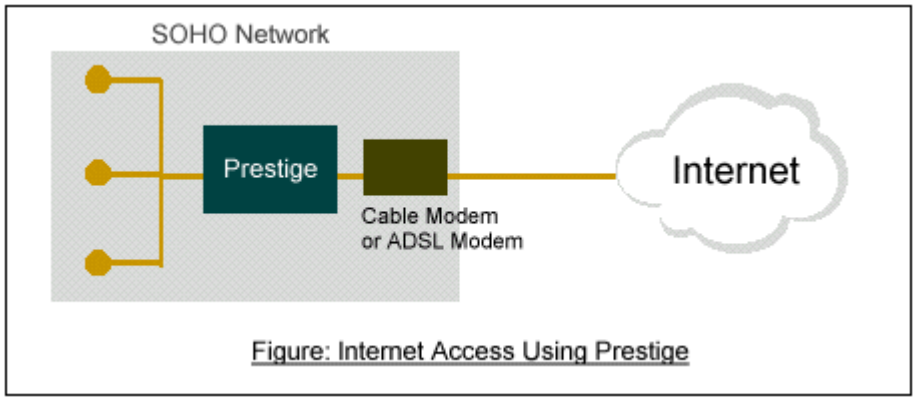


Figure: Internet Access Using Prestige

- Before you begin

The ZyXEL device is shipped with the following factory default:

1. IP address = 192.168.1.1, subnet mask = 255.255.255.0 (24 bits)
2. DHCP server enabled with IP pool starting from 192.168.1.33
3. Default SMT menu password = 1234

- Setting up the PC (Windows OS)

1. Ethernet connection

All PCs must have an Ethernet adapter card installed.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

- If you only have one PC, connect the PC's Ethernet adapter to the ZyXEL device's LAN port with a crossover (red one) Ethernet cable.
- If you have more than one PC, both the PC's Ethernet adapters and the ZyXEL device's LAN port must be connected to an external hub with straight Ethernet cable.

2. TCP/IP Installation

You must first install TCP/IP software on each PC before you can use it for Internet access. If you have already installed TCP/IP, go to the next section to configure it; otherwise, follow these steps to install:

- In the **Control Panel/Network** window, click **Add** button.
- In the **Select Network Component Type** windows, select **Protocol** and click **Add**.
- In the **Select Network Protocol** windows, select **Microsoft** from the manufacturers, then select **TCP/IP** from the **Network Protocols** and click **OK**.

3. TCP/IP Configuration

Follow these steps to configure Windows TCP/IP:

- In the **Control Panel/Network** window, click the **TCP/IP** entry to select it and click **Properties** button.
- In the **TCP/IP** Properties window, select **obtain an IP address automatically**.

Note: Do not assign arbitrary IP address and subnet mask to your PCs, otherwise, you will not be able to access the Internet.

- Click the **WINS** configuration tab and select **Disable WINS Resolution**.
- Click the **Gateway** tab. Highlight any installed gateways and click the **Remove** button until there are none listed.
- Click the **DNS Configuration** tab and select **Disable DNS**.
- Click **OK** to save and close the **TCP/IP** properties window
- Click **OK** to close the Network window. You will be prompted to insert your Windows CD or disk. When the drivers are updated, you will be asked if you want to restart the PC. Make sure your Prestige is powered on before answering Yes to the prompt. Repeat the above steps for each Windows PC on your network.

- **Setting up the ZyXEL router**

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

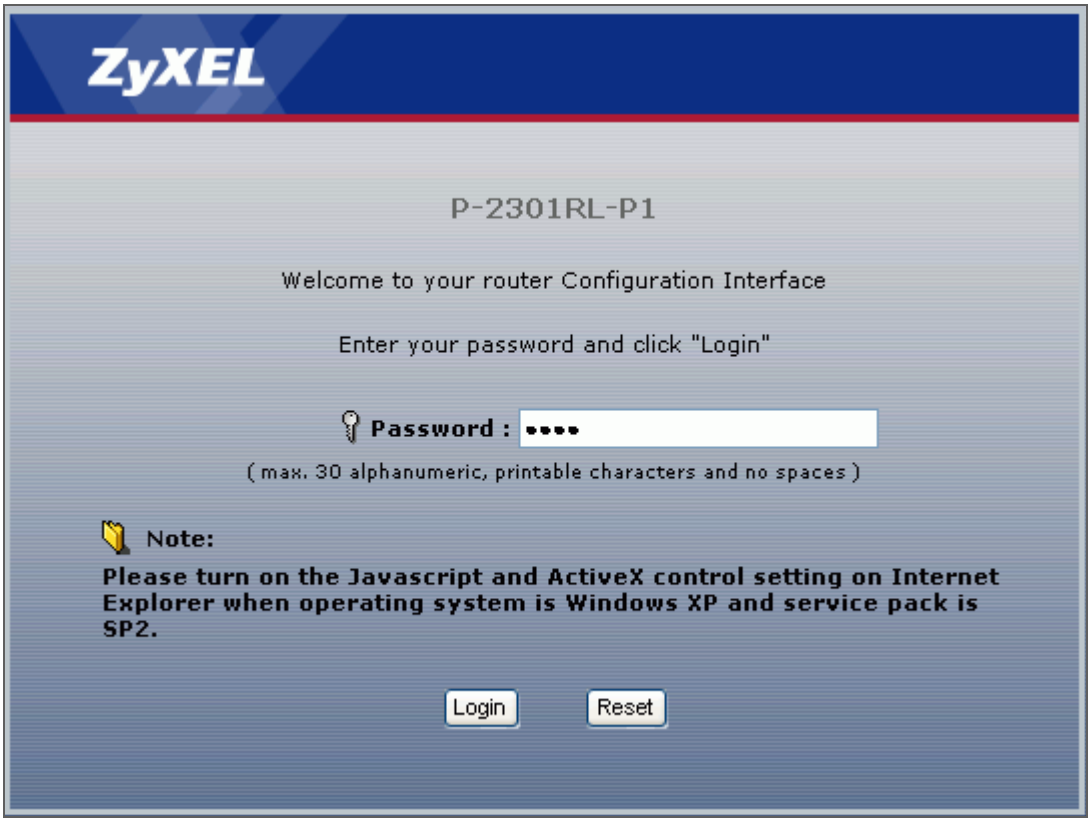
The following procedure is for the most typical usage of the ZyXEL device where you have a single-user account (SUA). The ZyXEL device supports embedded web server that allows you to use Web browser to configure it. Before configuring the router using Browser please be sure there is no Telnet or Console login.

1. Retrieve Prestige Web

Please enter the LAN IP address of the ZyXEL router in the URL location to retrieve the web screen from the ZyXEL device. The default LAN IP of the ZyXEL device is 192.168.1.1. See the example below. Note that you can either use http://192.168.1.1 or https://192.168.1.1

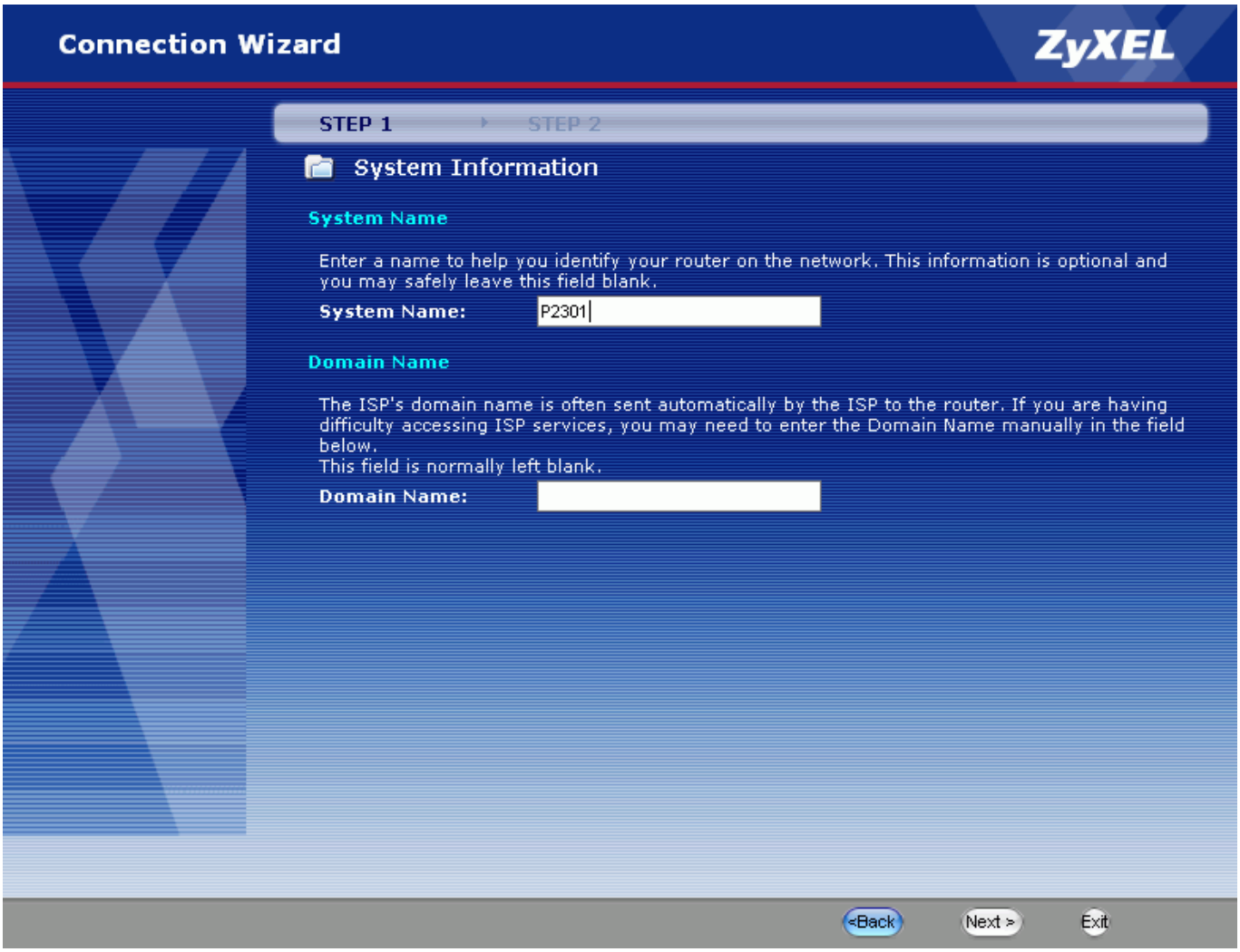
2. Login first

The default password is same as the default SMT password '1234'.


ZyXEL
P-2301RL-P1
Welcome to your router Configuration Interface
Enter your password and click "Login"
Password :
(max. 30 alphanumeric, printable characters and no spaces)
Note:
Please turn on the Javascript and ActiveX control setting on Internet Explorer when operating system is Windows XP and service pack is SP2.
Login
Reset

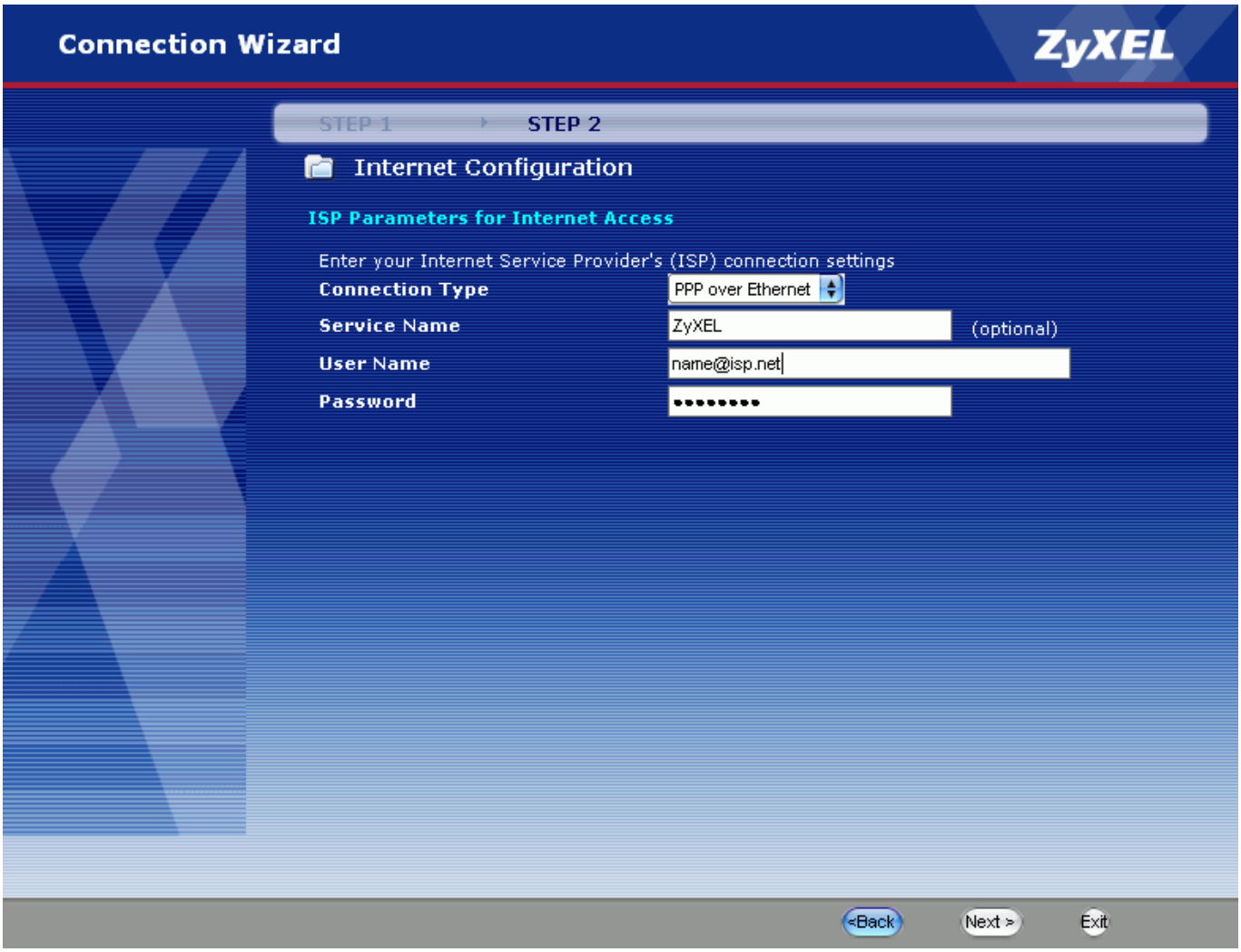
All contents Copyright (c) 2007 ZyXEL Communications Corporation.

3. Configures Internet access by using WIZARD SETUP


Connection Wizard
ZyXEL
STEP 1
STEP 2
System Information
System Name
Enter a name to help you identify your router on the network. This information is optional and you may safely leave this field blank.
System Name:
P2301
Domain Name
The ISP's domain name is often sent automatically by the ISP to the router. If you are having difficulty accessing ISP services, you may need to enter the Domain Name manually in the field below.
This field is normally left blank.
Domain Name:
<Back
Next >
Exit

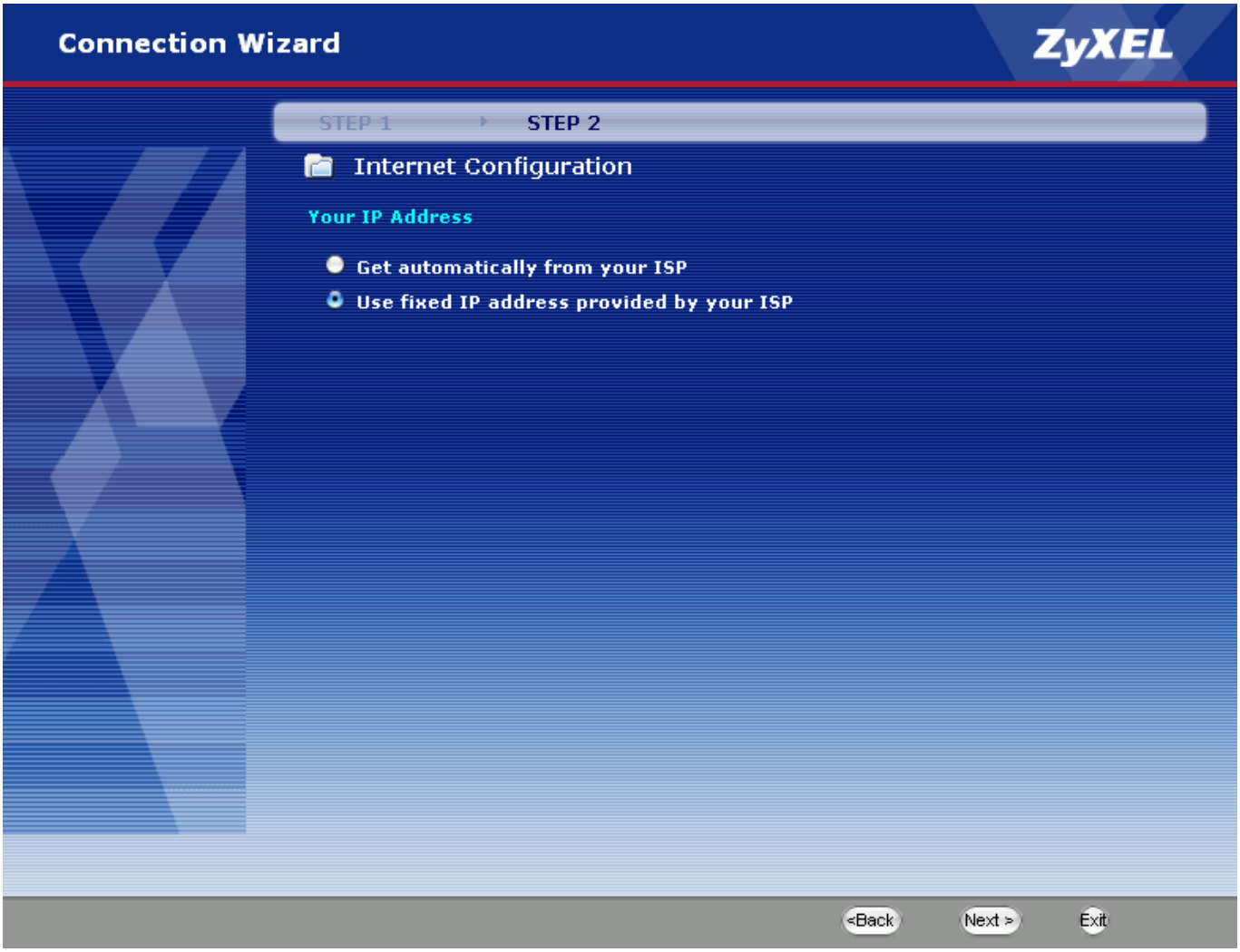
All contents Copyright (c) 2007 ZyXEL Communications Corporation.

The Web screen shown below takes PPPoE as the example.



All contents Copyright (c) 2007 ZyXEL Communications Corporation.

Select "Dynamic" if the ISP provides the IP dynamically, otherwise select "Use Fixed IP address" and enter the static IP given by ISP in the box following "MY WAN IP Address" field.



Setup the ZyXEL device as a DHCP Relay

- What is DHCP Relay?

DHCP stands for Dynamic Host Configuration Protocol. In addition to the DHCP server feature, the P2602 supports the DHCP relay function. When it is configured as DHCP server, it assigns the IP addresses to the

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

LAN clients. When it is configured as DHCP relay, it is reponsable for forwarding the requests and responses negotiating between the DHCP clients and the server. See figure 1.

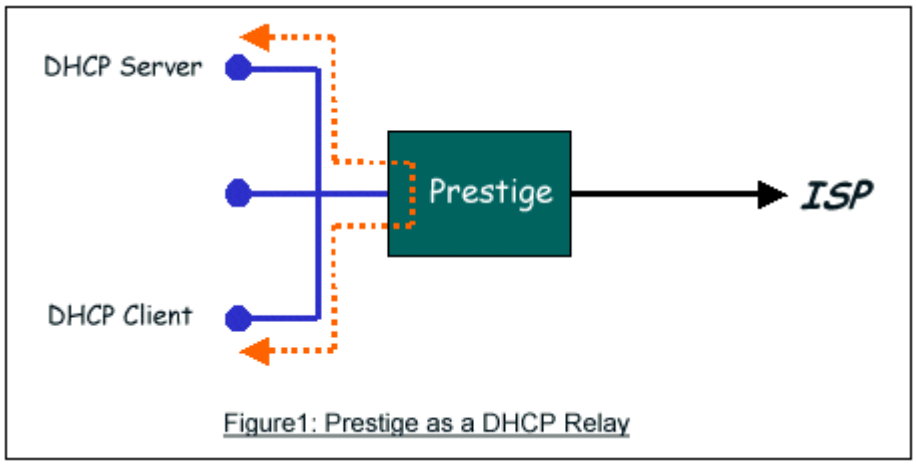


Figure1: Prestige as a DHCP Relay

- Setup the ZyXEL device as a DHCP Client

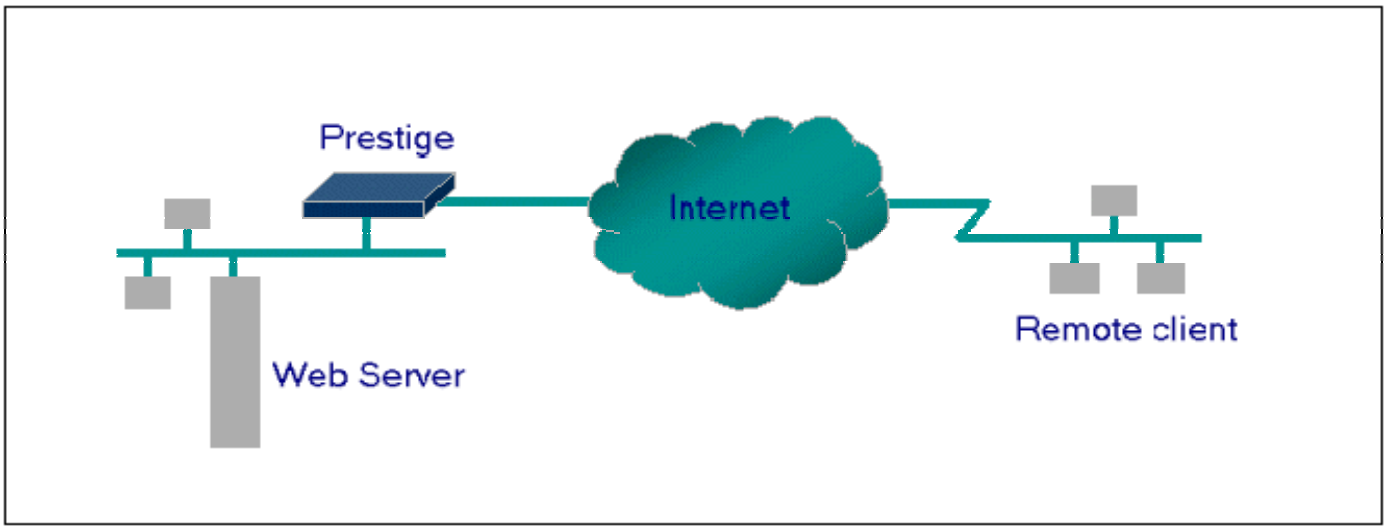
1. Toggle the DHCP to Relay in menu 3.2 and enter the IP address of the DHCP server in the **'Relay Server Address'** field.

```
                Menu 3.2 - TCP/IP and DHCP Ethernet Setup

DHCP= Relay                          TCP/IP Setup:
Client IP Pool:
  Starting Address= N/A              IP Address= 192.168.1.1
  Size of Client IP Pool= N/A        IP Subnet Mask= 255.255.255.0
First DNS Server= N/A                RIP Direction= Both
  IP Address= N/A                      Version= RIP-1
Second DNS Server= N/A               Multicast= None
  IP Address= N/A                    Edit IP Alias= No
Third DNS Server= N/A
  IP Address= N/A
DHCP Server Address= 192.168.1.2
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
Press ENTER to Confirm or ESC to Cancel:
```

Configure an Internal Server Behind SUA



- Introduction

If you wish, you can make internal servers (e.g., Web, ftp or mail server) accessible for outside users, even though SUA makes your LAN appear as a single machine to the outside world. A service is identified by the port number. Also, since you need to specify the IP address of a server in the ZyXEL device, a server must have a fixed IP address and not be a DHCP client whose IP address potentially changes each time it is powered on.

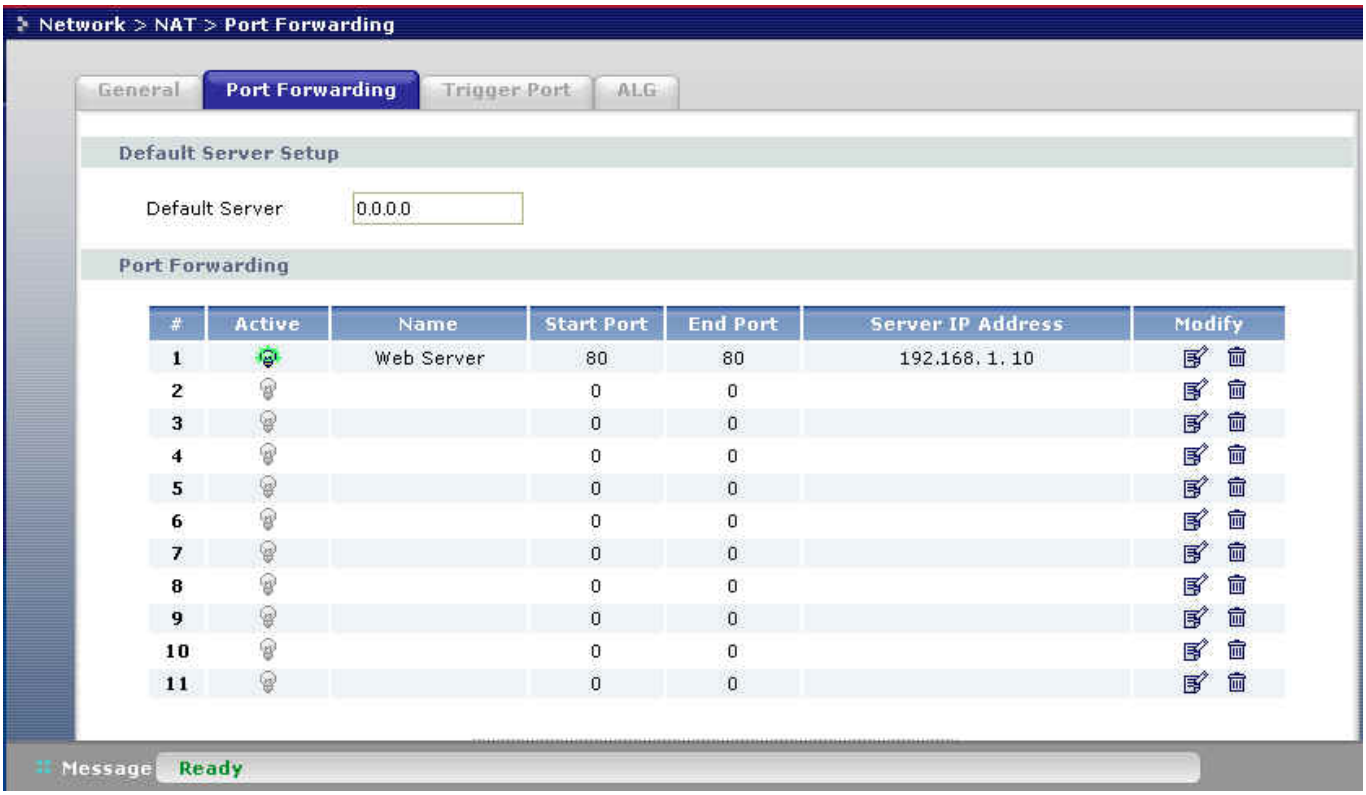
In addition to the servers for specific services, SUA supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default server is not defined, the service request is simply discarded.

- Configuration

To make a server visible to the outside world, specify the port number of the service and the inside address of the server in 'Menu 15.2.1', Multiple Server Configuration. The outside users can access the local server using the ZyXEL device's *WAN IP* address which can be obtained from menu 24.1.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

- For example (Configuring an internal Web server for outside access) :



- Port numbers for some services

Service	Port Number
FTP	21
Telnet	23
SMTP	25
DNS (Domain Name Server)	53
www-http (Web)	80

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

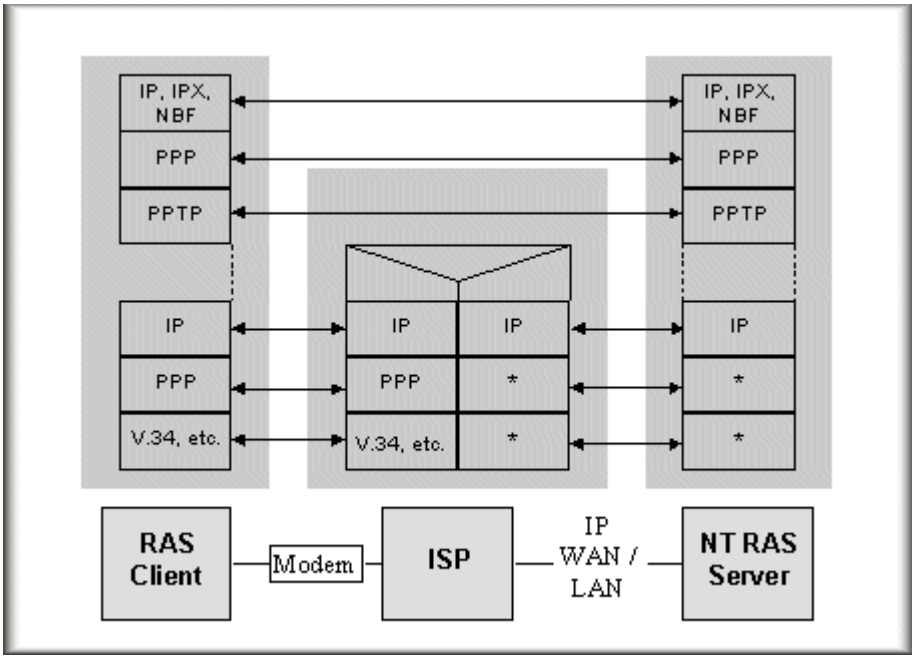
Configure a PPTP server Behind SUA

- Introduction

PPTP is a tunneling protocol defined by the PPTP forum that allows PPP packets to be encapsulated within Internet Protocol (IP) packets and forwarded over any IP network, including the Internet itself.

In order to run the Windows 9x PPTP client, you must be able to establish an IP connection with a tunnel server such as the Windows NT Server 4.0 Remote Access Server.

Windows Dial-Up Networking uses the Internet standard Point-to-Point (PPP) to provide a secure,optimized multiple-protocol network connection over dial-up telephone lines. All data sent over this connection can be encrypted and compressed, and multiple network level protocols (TCP/IP, NetBEUI and IPX) can be run correctly. Windows NT Domain Login level security is preserved even across the Internet.



Window98 PPTP Client / Internet / NT RAS Server Protocol Stack

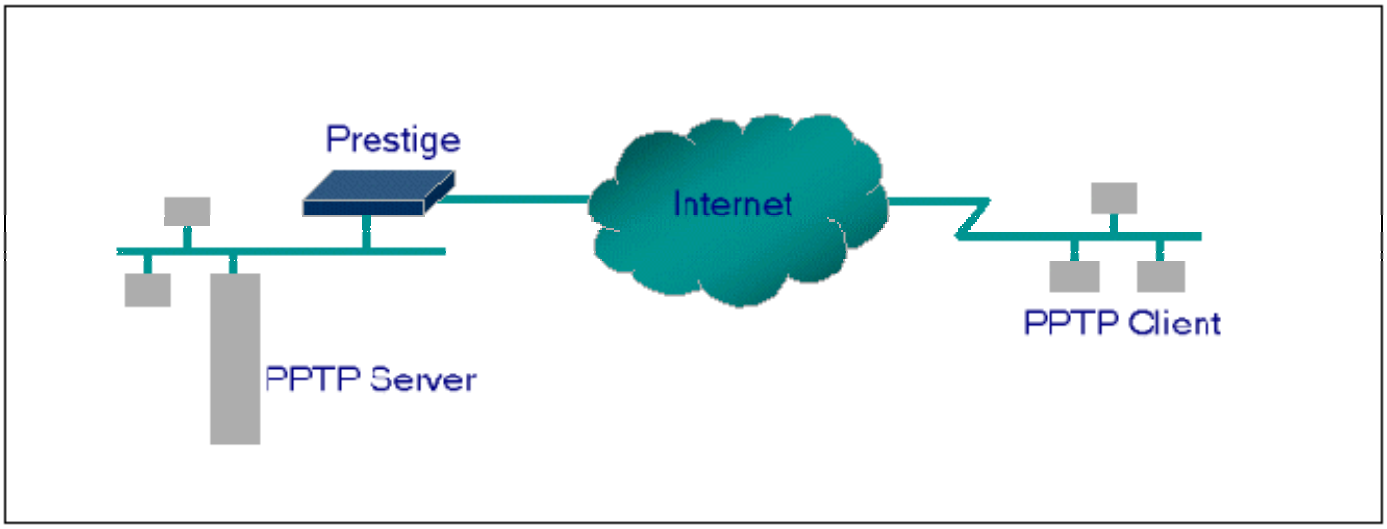
PPTP appears as new modem type (Virtual Private Networking Adapter) that can be selected when setting up a connection in the Dial-Up Networking folder. The VPN Adapter type does not appear elsewhere in the system. Since PPTP encapsulates its data stream in the PPP protocol, the VPN requires a second dial-up adapter. This second dial-up adapter for VPN is added during the installation phase of the Upgrade in addition to the first dial-up adapter that provides PPP support for the analog or ISDN modem.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

The PPTP is supported in Windows NT and Windows 98 already. For Windows 95, it needs to be upgraded by the Dial-Up Networking 1.2 upgrade.

- Configuration

This application note explains how to establish a PPTP connection with a remote private network in the ZyXEL device SUA case. In ZyNOS, all PPTP packets can be forwarded to the internal PPTP Server (WinNT server) behind SUA. The port number of the PPTP has to be entered in the SMT Menu 15 for Prestige to forward to the appropriate private IP address of Windows NT server.



- Example

The following example shows how to dial to an ISP via the ZyXEL device and then establish a tunnel to a private network. There will be three items that you need to set up for PPTP application, these are PPTP server (WinNT), PPTP client (Win9x) and the ZyXEL device.

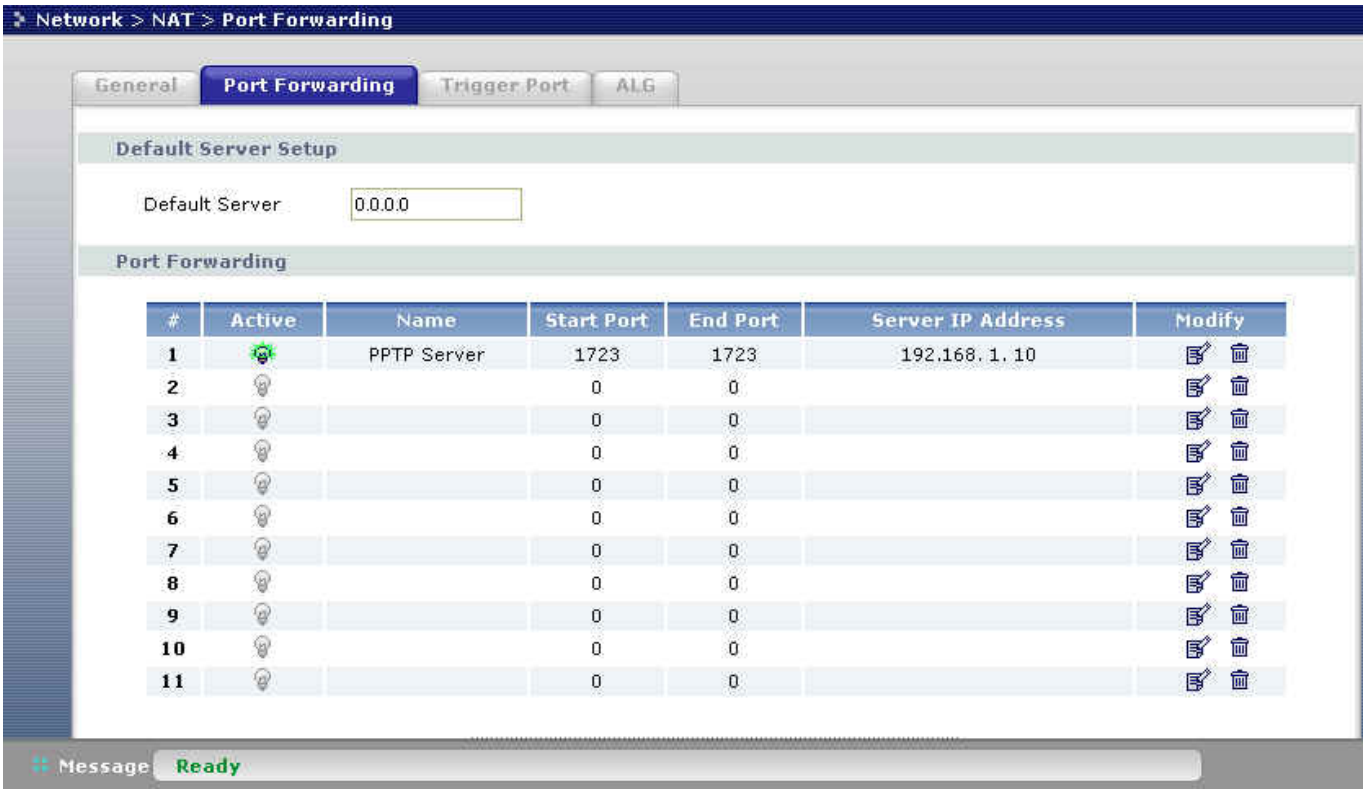
- PPTP server setup (WinNT)
  - Add the VPN service from Control Panel>Network
  - Add an user account for PPTP logged on user
  - Enable RAS port
  - Select the network protocols from RAS such as IPX, TCP/IP NetBEUI
  - Set the Internet gateway to Prestige
- PPTP client setup (Win9x)

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

- Add one VPN connection from Dial-Up Networking by entering the correct username & password and the IP address of the ZyXEL device's Internet IP address for logging to NT RAS server.
- Set the Internet gateway to the router that is connecting to ISP

o Prestige router setup

- Before making a VPN connection from Win9x to WinNT server, you need to connect Prestige router to your ISP first.
- Enter the IP address of the PPTP server (WinNT server) and the port number for PPTP as shown below.



When you have finished the above settings, you can ping to the remote Win9x client from WinNT. This ping command is used to demonstrate that remote the Win9x can be reached across the Internet. If the Internet connection between two LANs is achieve, you can place a VPN call from the remote Win9x client.

For example:

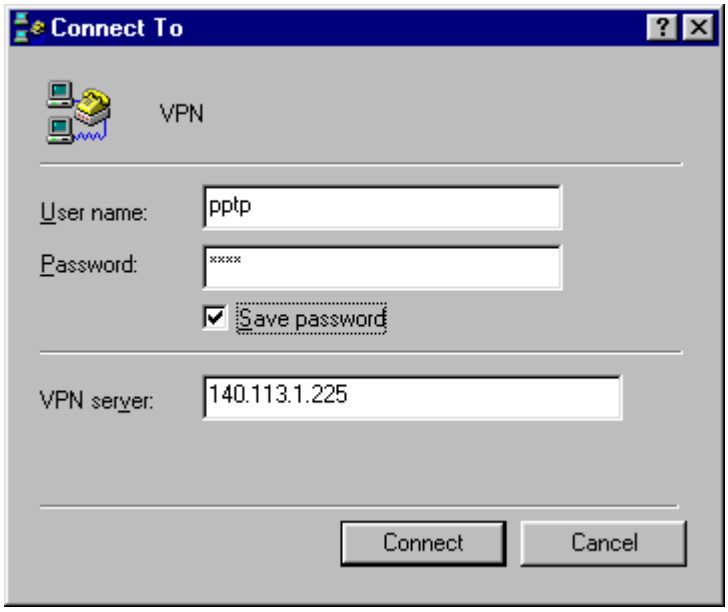
All contents Copyright (c) 2007 ZyXEL Communications Corporation.

C:\ping 203.66.113.2

When a dial-up connection to ISP is established, a default gateway is assigned to the router traffic through that connection. Therefore, the output below shows the default gateway of the Win9x client after the dial-up connection has been established.

Before making a VPN connection from the Win9x client to the NT server, you need to know the exact Internet IP address that the ISP assigns to Prestige router in SUA mode and enter this IP address in the VPN dial-up dialog box. You can check this Internet IP address from PNC Monitor or SMT Menu 24.1. If the Internet IP address is a fixed IP address provided by ISP in SUA mode, then you can always use this IP address for reaching the VPN server.

In the following example, the IP address '140.113.1.225' is dynamically assigned by ISP. You must enter this IP address in the 'VPN Server' dialog box for reaching the PPTP server. After the VPN link is established, you can start the network protocol application such as IP, IPX and NetBEUI.



All contents Copyright (c) 2007 ZyXEL Communications Corporation.

About Filter & Filter Examples

How does ZyXEL filter work?

- **Filter Structure**

The ZyXEL device allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port. The following diagram illustrates the logic flow when executing a filter rule.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

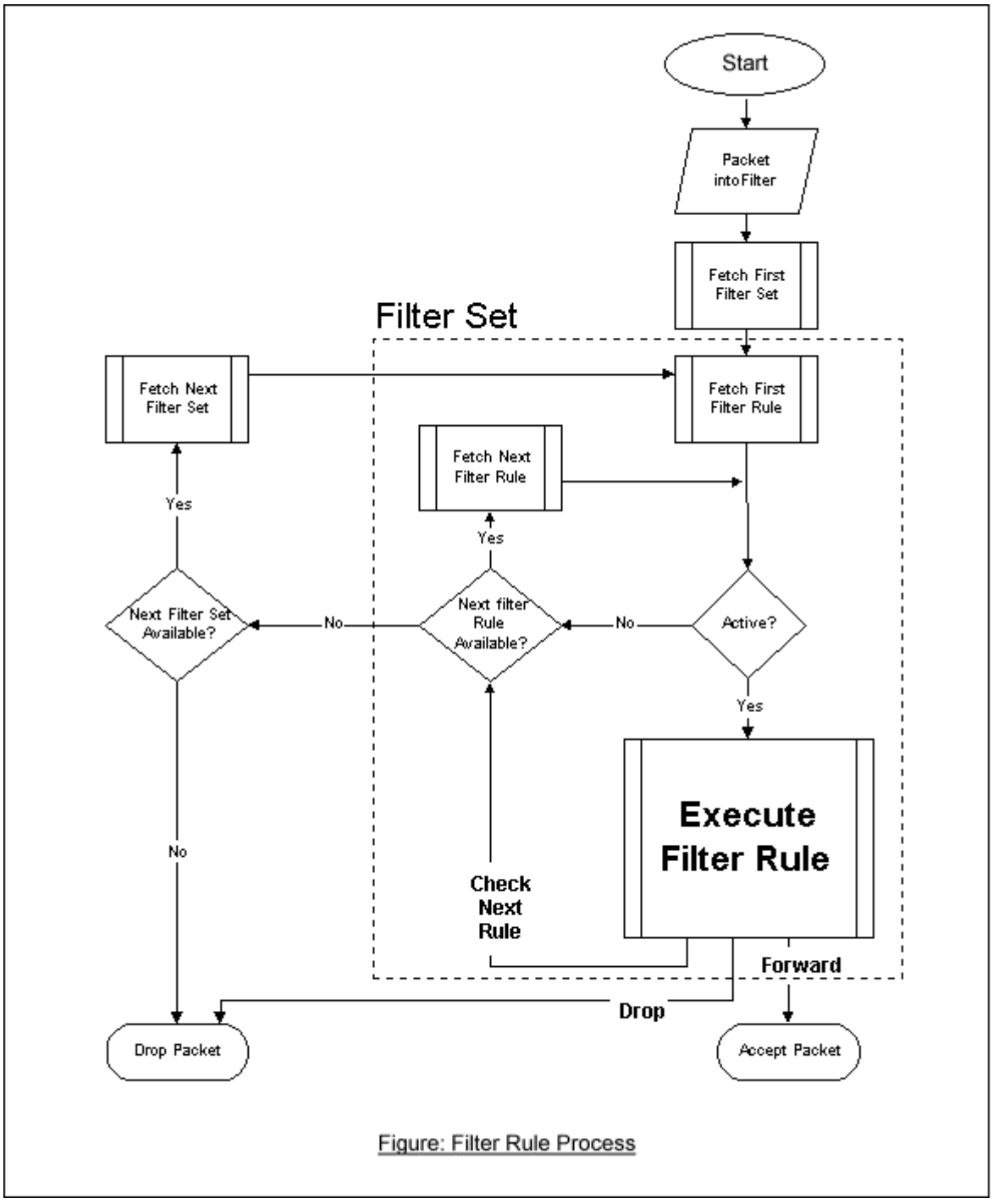


Figure: Filter Rule Process

- **Filter Types and SUA**

Conceptually, there are two categories of filter rules: device and protocol. The Generic filter rules belong to the

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

device category; they act on the raw data from/to LAN and WAN. The IP and IPX filter rules belong to the protocol category; they act on the IP and IPX packets.

In order to allow users to specify the local network IP address and port number in the filter rules with SUA connections, the TCP/IP filter function has to be executed before SUA for WAN outgoing packets and after the SUA for WAN incoming IP packets. But at the same time, the Generic filter rules must be applied at the point when the ZyXEL device is receiving and sending the packets; i.e. the ISDN interface. So, the execution sequence has to be changed. The logic flow of the filter is shown in Figure 1 and the sequence of the logic flow for the packet from LAN to WAN is:

- LAN device and protocol input filter sets.
- WAN protocol call and output filter sets.
- If SUA is enabled, SUA converts the source IP address from 192.168.1.33 to 203.205.115.6 and port number from 1023 to 4034.
- WAN device output and call filter sets.

The sequence of the logic flow for the packet from WAN to LAN is:

- WAN device input filter sets.
- If SUA is enabled, SUA converts the destination IP address from 203.205.115.6 to 92.168.1.33 and port number from 4034 to 1023.
- WAN protocol input filter sets.
- LAN device and protocol output filter sets.

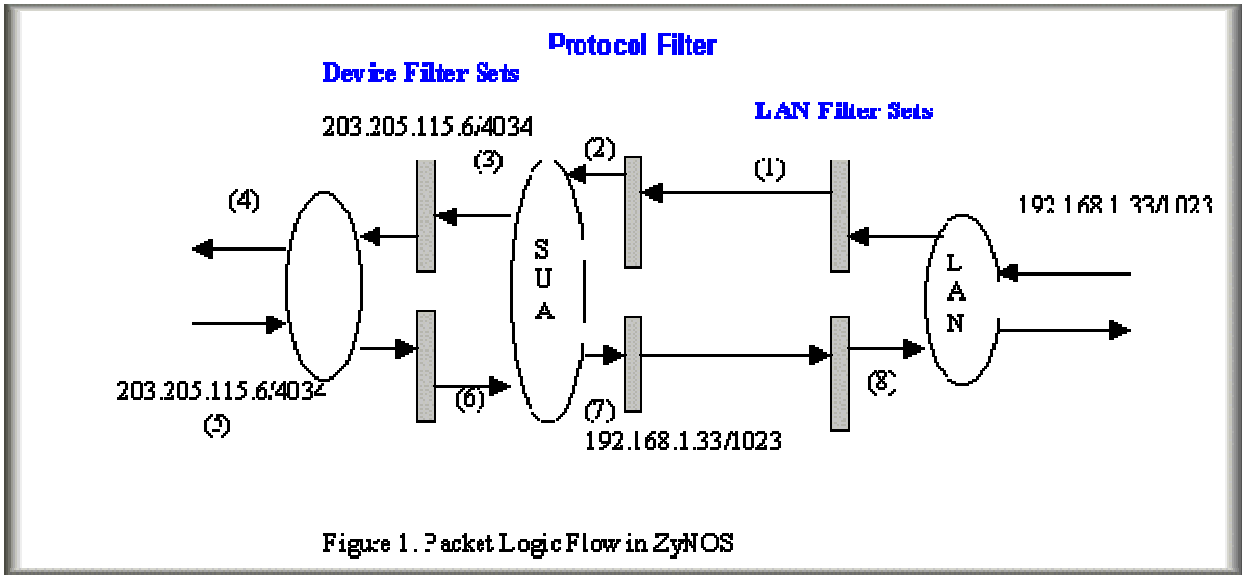


Figure 1. Packet Logic Flow in ZyNOS

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

Generic and TCP/IP (and IPX) filter rules are in different filter sets. The SMT will detect and prevent the mixing of different category rules within any filter set in Menu 21. In the following example, you will receive an error message 'Protocol and device filter rules cannot be active together' if you try to activate a TCP/IP (or IPX) filter rule in a filter set that has already had one or more active Generic filter rules. You will receive the same error if you try to activate a Generic filter rule in a filter set that has already had one or more active TCP/IP (or IPX) filter rules.

Menu 21.1.1:

```
          Menu 21.1.1 - Generic Filter Rule
Filter #: 1,1
Filter Type= Generic Filter Rule
Active= Yes
Offset= 0
Length= 0
Mask= N/A
Value= N/A
More= No            Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule
```

Menu 21.1.2:

```
          Menu 21.1.2 - TCP/IP Filter Rule
Filter #: 1,2
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 0    IP Source Route= No
Destination: IP Addr= 0.0.0.0
             IP Mask= 0.0.0.0
             Port #= 0
             Port # Comp= None
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
                    Source: IP Addr= 0.0.0.0
                            IP Mask= 0.0.0.0
                            Port #= 0
                            Port # Comp= None
                TCP Estab= N/A
                More= No          Log= None
                Action Matched= Check Next Rule
                Action Not Matched= Check Next Rule

                Press ENTER to Confirm or ESC to Cancel:
Saving to ROM.  Please wait...
Protocol and device rule cannot be active together
```

To separate the device and protocol filter categories; two new menus, Menu 11.5 and Menu 13.1, have been added, as well as some changes made to the Menu 3.1, Menu 11.1, and Menu 13. The new fields are shown below.

Menu 3.1:

```
                Menu 3.1 - General Ethernet Setup
                Input Filter Sets:
                  protocol filters=
                    device filters=
                Output Filter Sets:
                  protocol filters=
                    device filters=
```

Menu 11.1:

```
                        Menu 11.1 - Remote Node Profile

            Rem Node Name= LAN                Route= IP
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
Active= Yes                          Bridge= No

Encapsulation= PPP                   Edit PPP Options= No
Incoming:                            Rem IP Addr= ?
Rem Login= test                      Edit IP/IPX/Bridge= No
Rem Password= ********
Outgoing:                            Session Options:
My Login= testt                        Edit Filter Sets= Yes
My Password= *****
Authen= CHAP/PAP
          Press ENTER to Confirm or ESC to Cancel:
```

Menu 11.5:

```
          Menu 11.5 - Remote Node Filter
     Input Filter Sets:
       protocol filters=
         device filters=
     Output Filter Sets:
       protocol filters=
         device filters=
```

SMT will also prevent you from entering a protocol filter set configured in Menu 21 to the device filters field in Menu 3.1, 11.5, or entering a device filter set to the protocol filters field. Even though SMT will prevent the inconsistency from being entered in ZyNOS, it is unable to resolve the intermixing problems existing in the filter sets that were configured before. Instead, when ZyNOS translates the old configuration into the new format, it will verify the filter rules and log the inconsistencies. Please check the system log (Menu 24.3.1) before putting your device into use.

In order to avoid operational problems later, the ZyXEL device will disable its routing/bridging functions if there is an inconsistency among its filter rules.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

Filter for blocking the web service

- Configuration

Before configuring a filter, you need to know the following information:

1. The outbound packet type (protocol & port number)
2. The source IP address

Generally, the outbound packets for Web service could be as following:

a. HTTP packet, TCP (06) protocol with port number 80
b. DNS packet, TCP (06) protocol with port number 53 or
c. DNS packet, UDP (17) protocol with port number 53

For all workstation on the LAN, the source IP address will be 0.0.0.0. Otherwise, you have to enter an IP Address for the workstation you want to block. See the procedure for configuring this filter below.

- Create a filter set in Menu 21, e.g., set 1
- Create three filter rules in Menu 21.1.1, Menu 21.1.2, Menu 21.1.3
  - Rule 1- block the HTTP packet, TCP (06) protocol with port number 80
  - Rule 2- block the DNS packet, TCP (06) protocol with port number 53
  - Rule 3- block the DNS packet, UDP (17) protocol with port number 53
- Apply the filter set in menu 4

1. Create a filter set in Menu 21

```
                Menu 21 - Filter Set Configuration
Filter                              Filter
Set #       Comments                Set #       Comments
------  -----------------           ------  -----------------
  1      Web Request                   7      _______________
  2      _______________               8      _______________
  3      _______________               9      _______________
  4      _______________              10      _______________
  5      _______________              11      _______________
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
6       _____________              12       _____________

                Enter Filter Set Number to Configure= 1
                Edit Comments=
                Press ENTER to Confirm or ESC to Cancel:
```

2. Rule one for (a). http packet, TCP(06)/Port number 80

```
                     Menu 21.1.1 - TCP/IP Filter Rule
                Filter #: 1,1
                Filter Type= TCP/IP Filter Rule
                Active= Yes
                IP Protocol= 6      IP Source Route= No
                Destination: IP Addr= 0.0.0.0
                             IP Mask= 0.0.0.0
                             Port #= 80
                             Port # Comp= Equal
                     Source: IP Addr= 0.0.0.0
                             IP Mask= 0.0.0.0
                             Port #=
                             Port # Comp= None
                TCP Estab= No
                More= No            Log= None
                Action Matched= Drop
                Action Not Matched= Check Next Rule
                Press ENTER to Confirm or ESC to Cancel:
```

3.Rule 2 for (b).DNS request, TCP(06)/Port number 53

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
                Menu 21.1.2 - TCP/IP Filter Rule
           Filter #: 1,2
           Filter Type= TCP/IP Filter Rule
           Active= Yes
           IP Protocol= 6      IP Source Route= No
           Destination: IP Addr= 0.0.0.0
                        IP Mask= 0.0.0.0
                        Port #= 53
                        Port # Comp= Equal
                Source: IP Addr= 0.0.0.0
                        IP Mask= 0.0.0.0
                        Port #=
                        Port # Comp= None
           TCP Estab= No
           More= No            Log= None
           Action Matched= Drop
           Action Not Matched= Check Next Rule
           Press ENTER to Confirm or ESC to Cancel:
```

4. Rule 3 for (c). DNS packet UDP(17)/Port number 53

```
                Menu 21.1.2 - TCP/IP Filter Rule
           Filter #: 1,2
           Filter Type= TCP/IP Filter Rule
           Active= Yes
           IP Protocol= 17      IP Source Route= No
           Destination: IP Addr= 0.0.0.0
                        IP Mask= 0.0.0.0
                        Port #= 53
                        Port # Comp= Equal
                Source: IP Addr= 0.0.0.0
                        IP Mask= 0.0.0.0
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
                              Port #=
                              Port # Comp= None
                    TCP Estab= No
                    More= No            Log= None
                    Action Matched= Drop
                    Action Not Matched= Forward
                    Press ENTER to Confirm or ESC to Cancel:
```

5. After the three rules are completed, you will see the rule summary in Menu 21.

```
                        Menu 21.1 - Filter Rules Summary
# A Type                    Filter Rules         M m n
- - ---- ----------------------------------- - - -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=80    N D N
2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=53    N D N
3 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0,DP=53    N D F
```

6. Apply the filter set to the 'Output Protocol Filter Set' in the remote node setup.

A filter for blocking a specific client

Configuration

1. Create a filter set in Menu 21, e.g., set 1

```
                      Menu 21 - Filter Set Configuration
   Filter                              Filter
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
Set #       Comments                Set #       Comments
------  ----------------            ------  ----------------
  1       Block a client              7       _______________
  2       _______________             8       _______________
  3       _______________             9       _______________
  4       _______________            10       _______________
  5       _______________            11       _______________
  6       _______________            12       _______________

             Enter Filter Set Number to Configure= 0
             Edit Comments=
             Press ENTER to Confirm or ESC to Cancel:
```

2. One rule for blocking all packets from this client

```
                  Menu 21.1.1 - TCP/IP Filter Rule
             Filter #: 1,1
             Filter Type= TCP/IP Filter Rule
             Active= Yes
             IP Protocol= 0      IP Source Route= No
             Destination: IP Addr= 0.0.0.0
                          IP Mask= 0.0.0.0
                          Port #=
                          Port # Comp= None
                  Source: IP Addr= 192.168.1.5
                          IP Mask= 255.255.255.255
                          Port #=
                          Port # Comp= None
             TCP Estab= N/A
             More= No            Log= None
             Action Matched= Drop
             Action Not Matched= Forward
             Press ENTER to Confirm or ESC to Cancel:
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

Key Settings:

Source IP addr.....Enter the client IP in this field
IP Mask.....here the IP mask is used to mask the bits of the IP address given in the 'Source IP Addr=' field, for one workstation it is 255.255.255.255.
Action Matched.....Set to 'Drop' to drop all the packets from this client
Action Not Matched.....Set to 'Forward' to allow the packets from other clients

3. Apply the filter set number '1' to the 'Output Protocol Filter Set' field in the remote node setup.

A filter for blocking a specific MAC address

This configuration example shows you how to use a Generic Filter to block a specific MAC address of the LAN.

Before you Begin

Before you configure the filter, you need to know the MAC address of the client first. The MAC address can be provided by the NICs. If there is the LAN packet passing through the ZyXEL device you can identify the uninteresting MAC address from the ZyXEL device's LAN packet trace. Please have a look at the following example to know the trace of the LAN packets.

```
ras> sys trcp channel enet0 bothway
ras> sys trcp sw on
Now a client on the LAN is trying to ping Prestige·····
ras> sys trcp sw off
ras> sys trcp disp
TIME:  37c060  enet0-RECV len:74 call=0
  0000: [00 a0 c5 01 23 45] [00 80 c8 4c ea 63] 08 00 45 00
  0010: 00 3c eb 0c 00 00 20 01 e3 ea ca 84 9b 5d ca 84
  0020: 9b 63 08 00 45 5c 03 00 05 00 61 62 63 64 65 66
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
  0030: 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
  0040: 77 61 62 63 64 65 66 67 68 69
TIME:  37c060  enet0-XMIT len:74 call=0
  0000: [00 80 c8 4c ea 63] [00 a0 c5 01 23 45] 08 00 45 00
  0010: 00 3c 00 07 00 00 fe 01 f0 ef ca 84 9b 63 ca 84
  0020: 9b 5d 00 00 4d 5c 03 00 05 00 61 62 63 64 65 66
  0030: 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
  0040: 77 61 62 63 64 65 66 67 68 69
```

The detailed format of the Ethernet Version II:

```
+ Ethernet Version II
    - Address: 00-80-C8-4C-EA-63 (Source MAC) ----> 00-A0-C5-23-45
      (Destination MAC)
    - Ethernet II Protocol Type: IP
+ Internet Protocol
    - Version (MSB 4 bits): 4
    - Header length (LSB 4 bits): 5
    - Service type: Precd=Routine, Delay=Normal, Thrput=Normal, Reli=Normal
    - Total length: 60 (Octets)
    - Fragment ID: 60172
    - Flags: May be fragmented, Last fragment, Offset=0 (0x00)
    - Time to live: 32 seconds/hops
    - IP protocol type: ICMP (0x01)
    - Checksum: 0xE3EA
    - IP address 202.132.155.93  (Source IP address) ---->
      202.132.155.99(Destination IP address)
    - No option
+ Internet Control Message Protocol
    - Type: 8 - Echo Request
    - Code: 0
    - Checksum: 0x455C
    - Identifier: 768
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
   - Sequence Number: 1280
   - Optional Data: (32 bytes)
```

Configurations

From the above first trace, we know a client is trying to ping request the ZyXEL router. And from the second trace, we know the ZyXEL router will send a reply to the client accordingly. The following sample filter will utilize the 'Generic Filter Rule' to block the MAC address [00 80 c8 4c ea 63].

1. First, from the incoming LAN packet we know the uninteresting source MAC address starts at the 7th Octet

```
TIME:  37c060  enet0-RECV len:74 call=0
  0000: [00 a0 c5 01 23 45] [00 80 c8 4c ea 63] 08 00 45 00
  0010: 00 3c eb 0c 00 00 20 01 e3 ea ca 84 9b 5d ca 84
  0020: 9b 63 08 00 45 5c 03 00 05 00 61 62 63 64 65 66
  0030: 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
  0040: 77 61 62 63 64 65 66 67 68 69
```

2. We are now ready to configure the 'Generic Filter Rule' as below.

```
                Menu 21.1.1 - Generic Filter Rule
                 Filter #: 1,1
                 Filter Type= Generic Filter Rule
                 Active= Yes
                 Offset= 6
                 Length= 6
                 Mask= ffffffffffff
                 Value= 0080c84cea63
                 More= No            Log= None
                 Action Matched= Drop
                 Action Not Matched= Forward
```

Key Settings:

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

- Generic Filter Ruls
  Set the 'Filter Type' to 'Generic Filter Rule'

- Active
  Turn 'Active' to 'Yes'

- Offset (in bytes)
  Set to '6' since the source MAC address starts at 7th octets we need to skip the first octets of the destination MAC address.

- Length (in bytes)
  Set to '6' since MAC address has 6 octets.

- Mask (in hexadecimal)
  Specify the value that the ZyXEL device will logically qualify (logical AND) the data in the packet.
  Since the Length is set to 6 octets the Mask for it should be 12 hexadecimal numbers. In this case, we intent to set to 'ffffffffffff' to mask the incoming source MAC address, [00 80 c8 4c ea 63].

- Value (in hexadecimal)
  Specify the MAC address **[00 80 c8 4c ea 63]** that the ZyXEL device should use to compare with the masked packet. If the result from the masked packet matches the 'Value', then the packet is considered matched.

- Action Matched=
  Enter the action you want if the masked packet matches the 'Value'. In this case, we will drop it.

- Action Not Matched=
  Enter the action you want if the masked packet does not match the 'Value'. In this case, we will forward it. If you want to configure more rules please select 'Check Next Rule' to start configuring the next new rule. However, please note that the 'Filter Type' must be also 'Generic Filter Rule' but not others. Because the Generic and TCPIP (IPX) filter rules must be in different filter sets.

```
                Menu 21.1.2 - Generic Filter Rule
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
Filter #: 1,2
Filter Type= Generic Filter Rule
Active= Yes
Offset= 6
Length= 6
Mask= ffffffffffff
Value= 0080c810234a
More= No            Log= None
Action Matched= Drop
Action Not Matched= Forward
```

You can now apply it to the 'General Ethernet Setup' in Menu 3.1. Please note that the 'Generic Filter' can only be applied to the 'Device Filter' but not the 'Protocol Filter' that is used for configuring the TCPIP and IPX filters.

```
Menu 3.1 - General Ethernet Setup
   Input Filter Sets:
     protocol filters=
       device filters= 1
   Output Filter Sets:
     protocol filters=
       device filters=
```

A filter for blocking the NetBIOS packets

- Introduction

The NETBIOS protocol is used to share a Microsoft comupter of a workgroup. For the security concern, the NetBIOS connection to a outside host is blocked by Prestige router as factory defaults. Users can remove the

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

filter sets applied to menu 3.1 and menu 4.1 for activating the NetBIOS services. The details of the filter settings are described as follows.

- Configuration

The packets need to be blocked are as follows. Please configure two filter sets with 4 and 2 rules respectively based on the following packets in SMT menu 21.

Filter Set 1:

- Rule 1-Destination port number 137 with protocol number 6 (TCP)
- Rule 2-Destination port number 137 with protocol number 17 (UDP)
- Rule 3-Destination port number 138 with protocol number 6 (TCP)
- Rule 4-Destination port number 138 with protocol number 17 (UDP)
- Rule 5-Destination port number 139 with protocol number 6 (TCP)
- Rule 6-Destination port number 139 with protocol number 17 (UDP)

Filter Set 2:

- Rule 1-Source port number 137, Destination port number 53 with protocol number 6 (TCP)
- Rule 2-Source port number 137, Destination port number 53 with protocol number 17 (UDP)

Before starting to set the filter rules, please enter a name for each filter set in the 'Comments' field first.

```
                Menu 21 - Filter Set Configuration
Filter                          Filter
Set #     Comments              Set #       Comments
------  ----------------        ------  ----------------
  1     NetBIOS_WAN               7     _______________
  2     NetBIOS_LAN               8     _______________
  3     _______________           9     _______________
  4     _______________          10     _______________
  5     _______________          11     _______________
  6     _______________          12     _______________
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
Enter Filter Set Number to Configure= 1
Edit Comments=
Press ENTER to Confirm or ESC to Cancel:
```

Configure the first filter set 'NetBIOS_WAN' by selecting the Filter Set number 1.

- Rule 1-Destination port number 137 with protocol number 6 (TCP)

```
     Menu 21.1.1 - TCP/IP Filter Rule
Filter #: 1,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
             IP Mask= 0.0.0.0
             Port #= 137
             Port # Comp= Equal
     Source: IP Addr= 0.0.0.0
             IP Mask= 0.0.0.0
             Port #= 0
             Port # Comp= None
TCP Estab= No
More= No            Log= None
Action Matched= Drop
    Action Not Matched= Check Next Rule
Press ENTER to Confirm or ESC to Cancel:
```

- Rule 2-Destination port number 137 with protocol number 17 (UDP)

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
     Menu 21.1.2 - TCP/IP Filter Rule
Filter #: 1,2
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 17    IP Source Route= No
Destination: IP Addr= 0.0.0.0
             IP Mask= 0.0.0.0
             Port #= 137
             Port # Comp= Equal
     Source: IP Addr= 0.0.0.0
             IP Mask= 0.0.0.0
             Port #= 0
             Port # Comp= None
TCP Estab= N/A
More= No           Log= None
Action Matched= Drop
Action Not Matched= Check Next Rule
Press ENTER to Confirm or ESC to Cancel:
```

- Rule 3-Destination port number 138 with protocol number 6 (TCP)

```
     Menu 21.1.3 - TCP/IP Filter Rule
Filter #: 1,3
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6     IP Source Route= No
Destination: IP Addr= 0.0.0.0
             IP Mask= 0.0.0.0
             Port #= 138
             Port # Comp= Equal
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
        Source: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port #= 0
                Port # Comp= None
    TCP Estab= No
    More= No            Log= None
    Action Matched= Drop
    Action Not Matched= Check Next Rule

    Press ENTER to Confirm or ESC to Cancel:
```

- Rule 4-Destination port number 138 with protocol number 17 (UDP)

```
        Menu 21.1.4 - TCP/IP Filter Rule
    Filter #: 1,4
    Filter Type= TCP/IP Filter Rule
    Active= Yes
    IP Protocol= 17     IP Source Route= No
    Destination: IP Addr= 0.0.0.0
                 IP Mask= 0.0.0.0
                 Port #= 138
                 Port # Comp= Equal
        Source: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port #= 0
                Port # Comp= None
    TCP Estab= N/A
    More= No            Log= None
    Action Matched= Drop
    Action Not Matched= Check Next Rule
    Press ENTER to Confirm or ESC to Cancel:
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

- Rule 5-Destination port number 139 with protocol number 6 (TCP)

```
          Menu 21.1.5 - TCP/IP Filter Rule
     Filter #: 1,5
     Filter Type= TCP/IP Filter Rule
     Active= Yes
     IP Protocol= 6      IP Source Route= No
     Destination: IP Addr= 0.0.0.0
                  IP Mask= 0.0.0.0
                  Port #= 139
                  Port # Comp= Equal
          Source: IP Addr= 0.0.0.0
                  IP Mask= 0.0.0.0
                  Port #= 0
                  Port # Comp= None
     TCP Estab= No
     More= No            Log= None
     Action Matched= Drop
     Action Not Matched= Check Next Rule
     Press ENTER to Confirm or ESC to Cancel:
```

- Rule 6-Destination port number 139 with protocol number 17 (UDP)

```
          Menu 21.1.6 - TCP/IP Filter Rule
     Filter #: 1,6
     Filter Type= TCP/IP Filter Rule
     Active= Yes
     IP Protocol= 17     IP Source Route= No
     Destination: IP Addr= 0.0.0.0
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
                              IP Mask= 0.0.0.0
                              Port #= 139
                              Port # Comp= Equal
                         Source: IP Addr= 0.0.0.0
                              IP Mask= 0.0.0.0
                              Port #= 0
                              Port # Comp= None
                    TCP Estab= N/A
                    More= No            Log= None
                    Action Matched= Drop
                    Action Not Matched= Forward

                    Press ENTER to Confirm or ESC to Cancel:
```

- After the first filter set is finished, you will get the complete rules summary as below.

```
            Menu 21.2 - Filter Rules Summary
# A Type                        Filter Rules             M m n
 - - ---- ------------------------------------------- - - -
 1 Y IP   Pr=6,  SA=0.0.0.0, DA=0.0.0.0, DP=137         N D N
 2 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=137         N D N
 3 Y IP   Pr=6,  SA=0.0.0.0, DA=0.0.0.0, DP=138         N D N
 4 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=138         N D N
 5 Y IP   Pr=6,  SA=0.0.0.0, DA=0.0.0.0, DP=139         N D N
 6 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=139         N D F
```

- Apply the first filter set 'NetBIOS_WAN' to the **'Output Protocol Filter'** in the remote node setup.

Configure the second filter set 'NetBIOS_LAN' by selecting the Filter Set number 2.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

- Rule 1-Source port number 137, Destination port number 53 with protocol number 6 (TCP)

```
     Menu 21.2.1 - TCP/IP Filter Rule
Filter #: 2,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
             IP Mask= 0.0.0.0
             Port #= 53
             Port # Comp= Equal
     Source: IP Addr= 0.0.0.0
             IP Mask= 0.0.0.0
             Port #= 137
             Port # Comp= Equal
TCP Estab= No
More= No            Log= None
Action Matched= Drop
Action Not Matched= Check Next Rule
Press ENTER to Confirm or ESC to Cancel:
```

- Rule 2-Source port number 137, Destination port number 53 with protocol number 17 (UDP)

```
     Menu 21.2.2 - TCP/IP Filter Rule
Filter #: 2,2
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 17     IP Source Route= No
Destination: IP Addr= 0.0.0.0
             IP Mask= 0.0.0.0
             Port #= 53
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
                        Port # Comp= Equal
                Source: IP Addr= 0.0.0.0
                        IP Mask= 0.0.0.0
                        Port #= 137
                        Port # Comp= Equal
             TCP Estab= N/A
             More= No            Log= None
             Action Matched= Drop
             Action Not Matched= Forward
             Press ENTER to Confirm or ESC to Cancel:
```

1. After the first filter set is finished, you will get the complete rules summary as below.

```
            Menu 21.2 - Filter Rules Summary
# A Type                Filter Rules                      M m n
- - ---- ------------------------------------------- - - -
1 Y IP   Pr=6,  SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53   N D N
2 Y IP   Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53   N D F
```

1. Apply the filter set 'NetBIOS_LAN' in the **'Input protocol filters='** in the Menu 3 for blocking the packets from LAN

```
            Menu 3.1 - General Ethernet Setup

             Input Filter Sets:
                protocol filters= 2
                  device filters=
             Output Filter Sets:
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
                protocol filters=
                  device filters=
```

Using the Dynamic DNS (DDNS)

1. What is DDNS?

The DDNS service, an IP Registry provides a public central database where information such as email addresses, hostnames, IPs etc. can be stored and retrieved. This solves the problems if your DNS server uses an IP associated with dynamic IPs.

Without DDNS, we always tell the users to use the WAN IP of the ZyXEL device to access the internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported by the ZyXEL device, you apply a DNS name (e.g., www.zyxel.com.tw) for your server (e.g., Web server) from a DDNS server. The outside users can always access the web server using the www.zyxel.com.tw regardless of the WAN IP of the ZyXEL device.

When the ISP assigns the ZyXEL device a new IP, the ZyXEL device must inform the DDNS server the change of this IP so that the server can update its IP-to-DNS entry. Once the IP-to-DNS table in the DDNS server is updated, the DNS name for your web server (i.e., www.zyxel.com.tw) is still usable.

The DDNS server stores password-protected email addresses with IPs and hostnames and accepts queries based on email addresses. So, there must be an email entry in the ZyXEL device menu 1.

The DDNS servers the ZyXEL device supports currently is WWW.DYNDNS.ORG where you apply the DNS from and update the WAN IP to.

- Setup the DDNS

- Before configuring the DDNS settings in the ZyXEL device, you must register an account from the DDNS server such as WWW.DYNDNS.ORG first. After the registration, you have a hostname for your internal server and a password using to update the IP to the DDNS server.
- Visit **'Dynamic DNS'** in the **'Maintenance>System'** in the WEB GUI to configure the settings.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

Key Settings for using DDNS function:

Option	Description
Service Provider	Enter the DDNS server in this field. Currently, we support WWW.DYNDNS.ORG.
Host	Enter the hostname you subscribe from the above DDNS server. For example, zyxel.com.tw.
User	Enter the user name that
Password	Enter the password that the DDNS server gives to you.
Enable Wildcard	Enter the hostname for the wildcard function that the WWW.DYNDNS.ORG supports. Note that Wildcard option is available only when the provider is WWW.DYNDNS.ORG.

Network Management Using SNMP

1. SNMP Overview

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

The *Simple Network Management Protocol* (SNMP) is an applications-layer protocol used to exchange the management information between network devices (e.g., routers). By using SNMP, network administrators can more easily manage network performance, find and solve network problems. The SNMP is a member of the TCP/IP protocol suite, it uses the UDP to exchange messages between a management Client and an Agent, residing in a network node.

There are two versions of SNMP: Version 1 and Version 2. ZyXEL supports SNMPv1. Most of the changes introduced in Version 2 increase SNMP's security capabilities. SNMP encompasses three main areas:

1. A small set of management operations.
2. Definitions of management variables.
3. Data representation.

The operations allowed are: Get, GetNext, Set, and Trap. These functions operates on variables that exist in network nodes. Examples of variables include statistic counters, node port status, and so on. All of the SNMP management functions are carried out through these simple operations. No action operations are available, but these can be simulated by the setting of flag variables. For example, to reset a node, a counter variable named 'time to reset' could be set to a value, causing the node to reset after the time had elapsed.

SNMP variables are defined using the OSI Abstract Syntax Notation One (ASN.1). ASN.1 specifies how a variable is encoded in a transmitted data frame; it is very powerful because the encoded data is self-defining. For example, the encoding of a text string includes an indication that the data unit is a string, along with its length and value. ASN.1 is a flexible way of defining protocols, especially for network management protocols where nodes may support different sets of manageable variables.

The net of variables that each node supports is called the *Management Information Base* (MIB). The MIB is made up of several parts, including the Standard MIB, specified as part of SNMP, and Enterprise Specific MIB, which are defined by different manufacturer for hardware specific management.

The current Internet-standard MIB, MIB-II, is defined in RFC 1213 and contains 171 objects. These objects are grouped by protocol (including TCP, IP, UDP, SNMP, and other categories, including 'system' and 'interface.'

The Internet Management Model is as shown in figure 1. Interactions between the NMS and managed devices can be any of four different types of commands:

6. Reads

   Read is used to monitor the managed devices, NMSs read variables that are maintained by the devices.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

7. Writes

   Write is used to control the managed devices, NMSs write variables that are stored in the managed devices.

8. Traversal operations

   NMSs use these operations to determine which variables a managed device supports and to sequentially gather information from variable tables (such as IP routing table) in managed devices.

9. Traps

The managed devices to asynchronously report certain events to NMSs use trap.

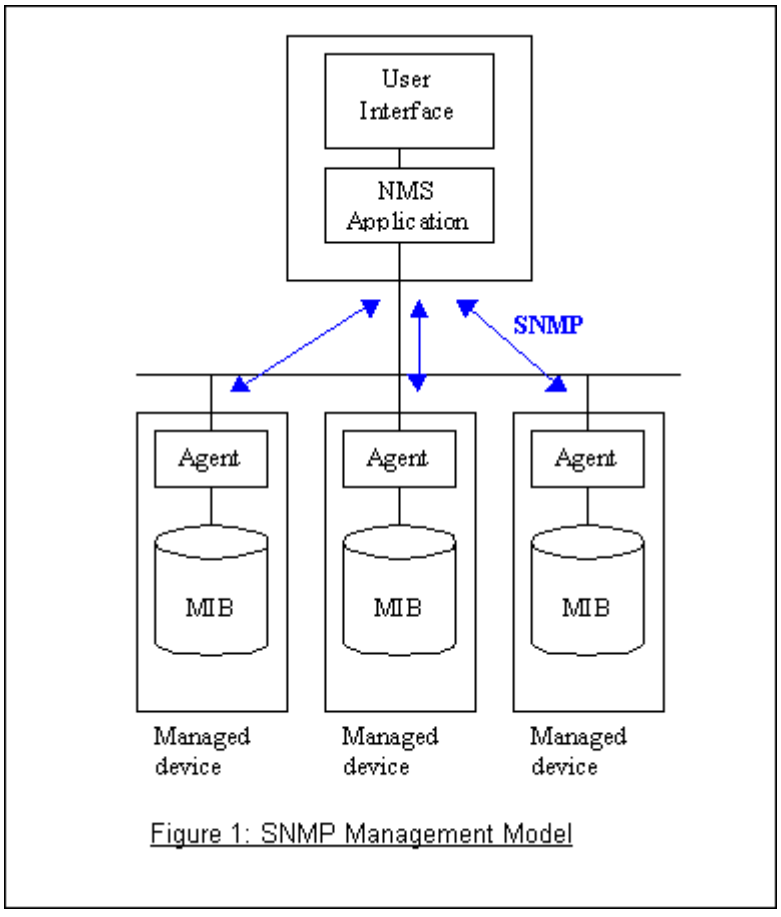


Figure 1: SNMP Management Model

2. SNMPv1 Operations

SNMP itself is a simple request/response protocol. 4 SNMPv1 operations are defined as below.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

- **Get**
  Allows the NMS to retrieve an object variable from the agent.
- **GetNext**
  Allows the NMS to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a NMS wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- **Set**
  Allows the NMS to set values for object variables within an agent.
- **Trap**
  Used by the agent to inform the NMS of some events.

The SNMPv1 messages contains two part. The first part contains a version and a community name. The second part contains the actual SNMP protocol data unit (PDU) specifying the operation to be performed (Get, Set, and so on) and the object values involved in the operation. The following figure shows the SNMPv1 message format.

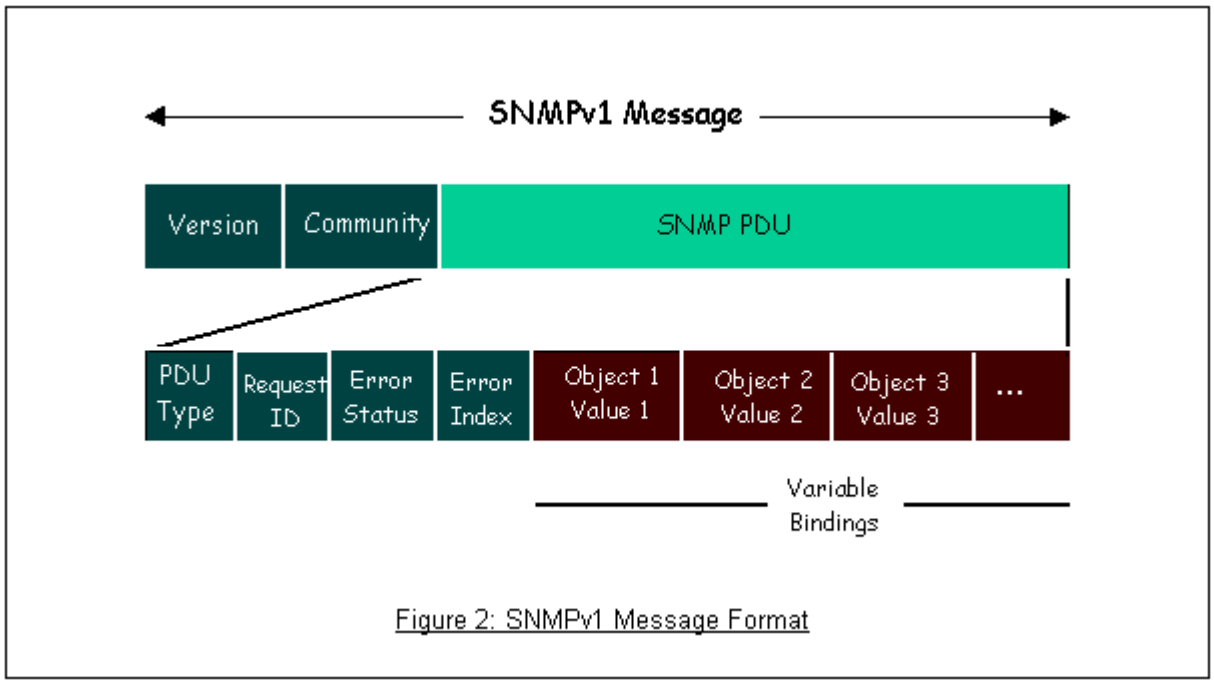


Figure 2: SNMPv1 Message Format

The SNMP PDU contains the following fields:

- **PDU type** Specifies the type of PDU.
- **Request ID** Associates requests with responses.
- **Error status** Indicates an error and an error type.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

- **Error index** Associates the error with a particular object variable.
- **Variable-bindings** Associates particular object with their value.

3. ZyXEL SNMP Implementation

ZyXEL currently includes SNMP support in some Prestige routers. It is implemented based on the SNMPv1, so it will be able to communicate with SNMPv1 NMSs. For SNMPv1 operation, ZyXEL permits one community string so that the router can belong to only one community and allows trap messages to be sent to only one NMS manager.

Some traps are sent to the SNMP manager when anyone of the following events happens:

- coldStart (defined in RFC-1215) :

  If the machine coldstarts, the trap will be sent after booting.

- warmStart (defined in RFC-1215) :

  If the machine warmstarts, the trap will be sent after booting.

- linkDown (defined in RFC-1215) :

  If any link of IDSL or WAN is down, the trap will be sent with the port number . The port number is its interface index under the interface group.

- linkUp (defined in RFC-1215) :

  If any link of IDSL or WAN is up, the trap will be sent with the port number . The port number is its interface index under the interface group.

- authenticationFailure (defined in RFC-1215) :

When receiving any SNMP get or set requirement with wrong community, this trap is sent to the manager.

1. whyReboot (defined in ZYXEL-MIB) :

When the system is going to restart (warmstart), the trap will be sent with the reason of restart before rebooting.

(i) For intentional reboot :

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

In some cases (download new files, CI command "sys reboot", ...), reboot is done intentionally. And traps with the message "System reboot by user !" will be sent.

(ii) For fatal error :

System has to reboot for some fatal errors. And traps with the message of the fatal code will be sent.

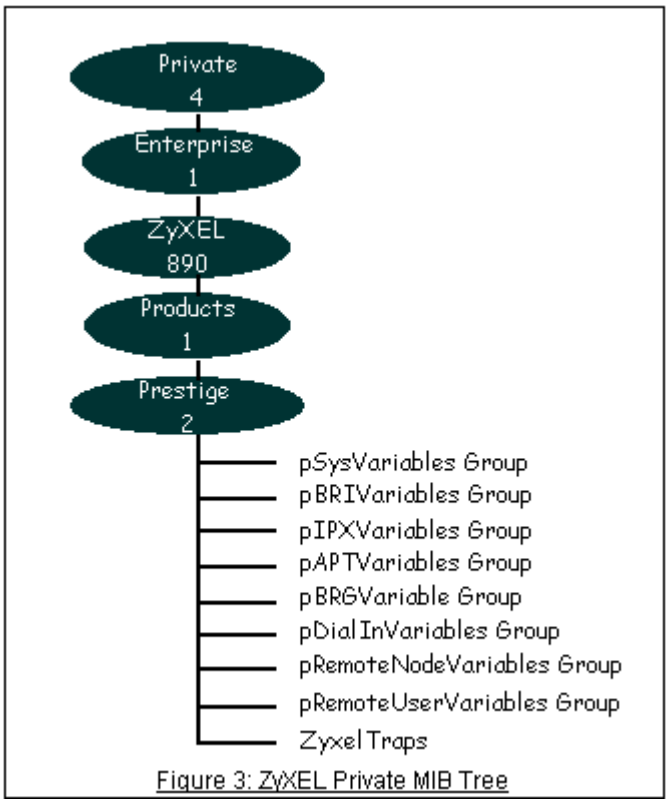
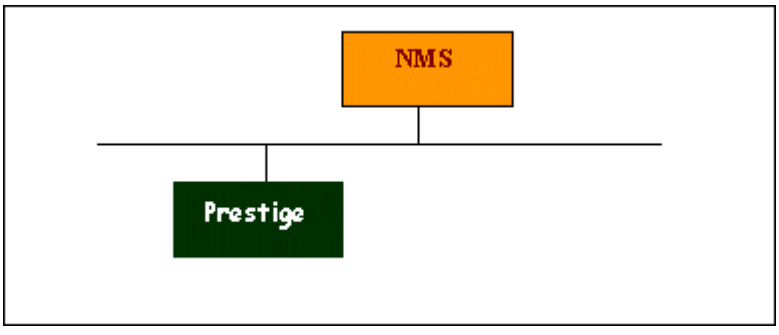


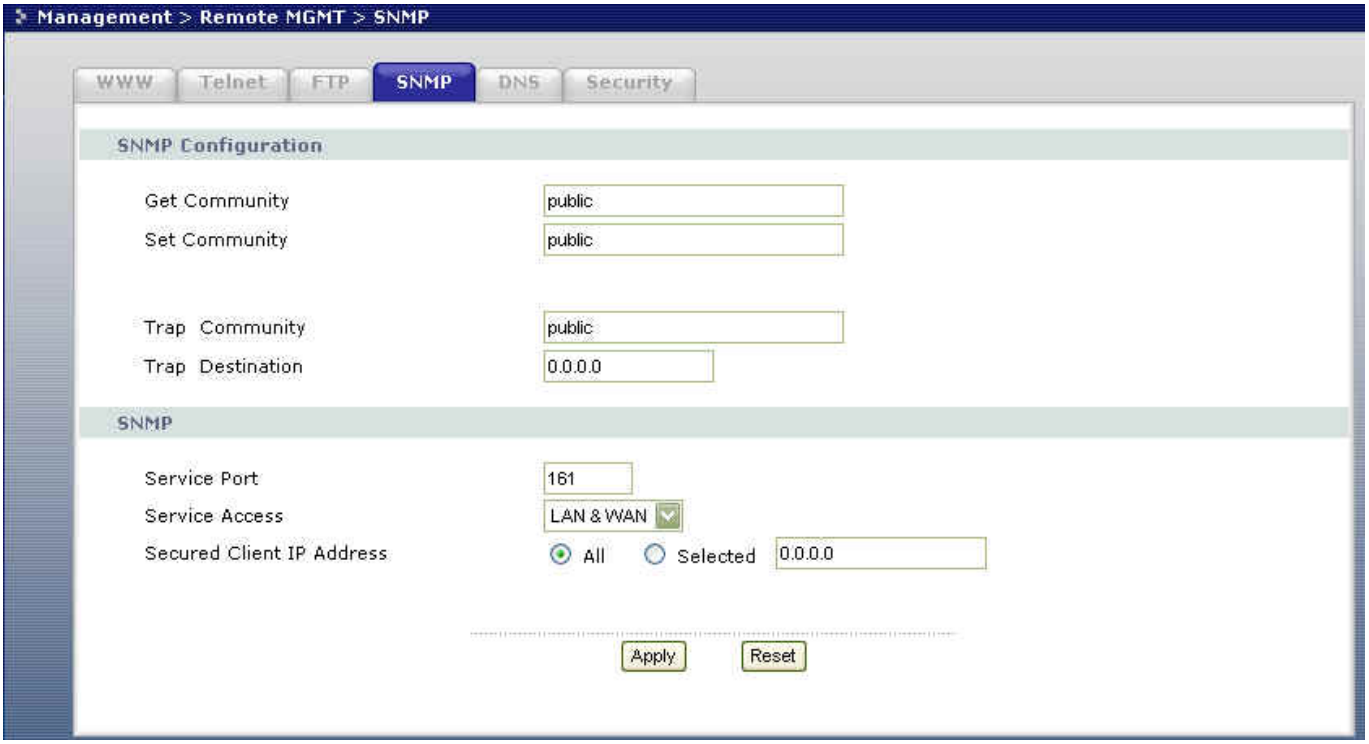
Figure 3: ZyXEL Private MIB Tree

4. Configure the ZyXEL device for SNMP



The SNMP related settings in Prestige are configured in menu 22, SNMP Configuration. The following steps describe a simple setup procedure for configuring all SNMP settings.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.



Key Settings:

Option	Descriptions
Get Community	Enter the correct Get Community. This Get Community must match the 'Get-' and 'GetNext' community requested from the NMS. The default is 'public'.
Set Community	Enter the correct Set Community. This Set Community must match the 'Set-community requested from the NMS. The default is 'public'.
Trusted Host	Enter the IP address of the NMS. The ZyXEL device will only respond to SNMP messages coming from this IP address. **If 0.0.0.0 is entered, the ZyXEL device will respond to all NMS managers.**
Trap Community	Enter the community name in each sent trap to the NMS. This Trap Community must match what the NMS is expecting. The default is 'public'.
Trap Destination	Enter the IP address of the NMS that you wish to send the traps to. **If 0.0.0.0 is entered, the ZyXEL device will not send trap any NMS manager.**

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

Using syslog

4. **Prestige Setup**

Configuration:

1. Active, use the space bar to turn on the syslog option.
2. Syslog IP Address, enter the IP address of the UNIX server that you wish to send the syslog.
3. Log Facility, use the space bar to toggle between the 7 different local options.

- **UNIX Setup**

1. Make sure that your syslogd starts with *-r* argument.

-r, this option will enable the facility to receive message from the network using an Internet domain socket with the syslog services. The default setting is not enabled.

2. Edit the file /etc/syslog.conf by adding the following line at the end of the /etc/syslog.conf file.

```
local1.*                /var/log/zyxel.log
```

Where /var/log/zyxel.log is the full path of the log file.

3. Restart syslogd.

- **CDR log**(call messages)

Format:

sdcmdSyslogSend(SYSLOG_CDR, SYSLOG_INFO, String);
String = board xx line xx channel xx, call xx, str

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

board = the hardware board ID
line = the WAN ID in a board
channel = channel ID within the WAN
call = the call reference number which starts from 1 and increments by 1 for each new call
str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)
C01 Incoming Call xxxxBps xxxxx (L2TP,xxxxx means Remote Call ID)
C01 Incoming Call xxxx (means connected speed) xxxxx (means Remote Call ID)
L02 Tunnel Connected(L2TP)
C02 OutCall Connected xxxx (means connected speed) xxxxx (means Remote Call ID)
C02 CLID call refused
L02 Call Terminated
C02 Call Terminated

Example:

```
Feb 14 16:57:17 192.168.1.1 ZyXEL Communications Corp.: board 0 line 0 channel 0, call 18, C01 Incoming Call OK
Feb 14 17:07:18 192.168.1.1 ZyXEL Communications Corp.: board 0 line 0 channel 0, call 18, C02 Call Terminated
```

- **Packet triggered log**

Format:

sdcmdSyslogSend(SYSLOG_PKTTRI, SYSLOG_NOTICE, String);
String = Packet trigger: Protocol=xx Data=xxxxxxxxxx
Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)
Data: We will send forty-eight Hex characters to the server

Example:

```
Jul 19 11:28:39 192.168.102.2 ZyXEL Communications Corp.: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f7071727374
Jul 19 11:28:56 192.168.102.2 ZyXEL Communications Corp.: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

- **Filter log**

This message is available when the 'Log' is enabled in the filter rule setting. The message consists of the packet header and the log of the filter rules.

Format:

sdcmdSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String);
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx]S04>R01mD
IP[...] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m) drop (D).
Src: Source Address
Dst: Destination Address
prot: Protocol (TCP,UDP,ICMP)
spo: Source port
dpo: Destination port

Example:

```
Jul 19 14:44:09 192.168.1.1 ZyXEL Communications Corp.: IP[Src=202.132.154.1 Dst=192.168.1.33 UDP
spo=0035  dpo=05d4]}S03>R01mF
Jul 19 14:44:13 192.168.1.1 ZyXEL Communications Corp.: IP[Src=192.168.1.33 Dst=202.132.154.1
ICMP]}S03>R01mF
```

- **PPP Log**

Format:

sdcmdSyslogSend(SYSLOG_PPPLOG, SYSLOG_NOTICE, String);
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown
Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP /IPXCP

Example:

```
Jul 19 11:43:25 192.168.1.1 ZyXEL Communications Corp.: ppp:LCP Starting
Jul 19 11:43:29 192.168.1.1 ZyXEL Communications Corp.: ppp:IPCP Starting
Jul 19 11:43:34 192.168.1.1 ZyXEL Communications Corp.: ppp:CCP Starting
```

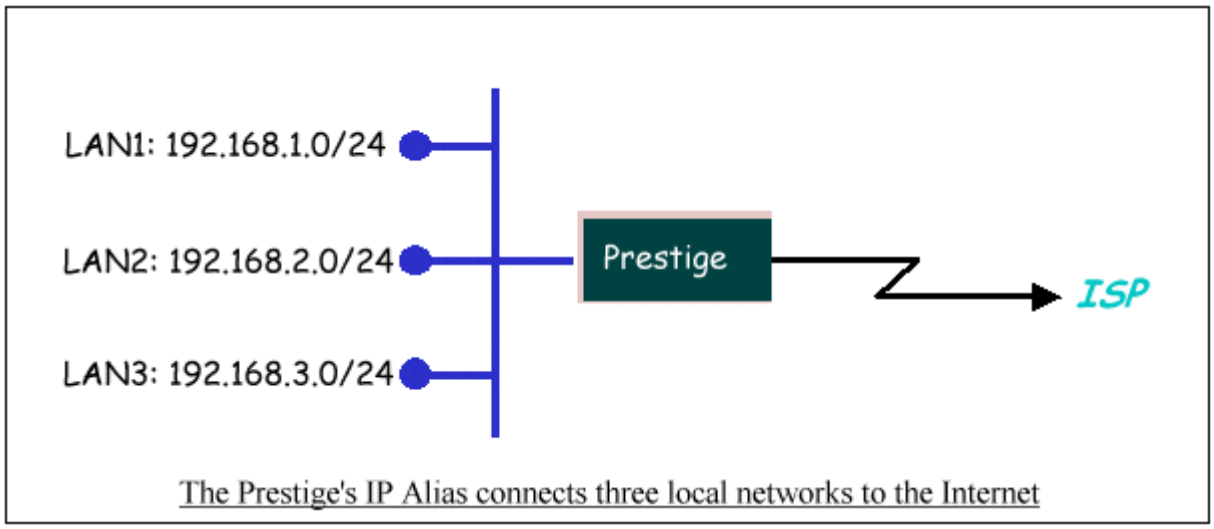
All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
Jul 19 11:43:38 192.168.1.1 ZyXEL Communications Corp.: ppp:BACP Starting
Jul 19 11:43:43 192.168.1.1 ZyXEL Communications Corp.: ppp:IPCP Opening
Jul 19 11:43:51 192.168.1.1 ZyXEL Communications Corp.: ppp:CCP Opening
Jul 19 11:43:55 192.168.1.1 ZyXEL Communications Corp.: ppp:BACP Opening
Jul 19 11:44:00 192.168.1.1 ZyXEL Communications Corp.: ppp:LCP Closing
Jul 19 11:44:05 192.168.1.1 ZyXEL Communications Corp.: ppp:IPCP Closing
Jul 19 11:44:09 192.168.1.1 ZyXEL Communications Corp.: ppp:CCP Closing
Jul 19 11:44:14 192.168.1.1 ZyXEL Communications Corp.: ppp:BACP Closing
```

Using IP Alias

- What is IP Alias ?

In a typical environment, a LAN router is required to connect two local networks. The ZyXEL device can connect three local networks to the ISP or a remote node, we call this function as 'IP Alias'. In this case, an internal router is not required. For example, the network manager can divide the local network into three networks and connect them to the Internet using Prestige's single user account. See the figure below.



The Prestige's IP Alias connects three local networks to the Internet

The ZyXEL device supports three virtual LAN interfaces via its single physical Ethernet interface. The first network can be configured in menu 3.2 as usual. The second and third networks that we call 'IP Alias 1' and 'IP Alias 2' can be configured in menu 3.2.1-IP Alias Setup.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

There are three internal virtual LAN interfaces for the ZyXEL device to route the packets from/to the three networks correctly. They are **enif0** for the major network, **enif0:0** for the IP alias 1 and **enif0:1** for the IP alias 2. Therefore, three routes are created in the ZyXEL device as shown below when the three networks are configured. If the ZyXEL device's DHCP is also enabled, the IP pool for the clients can be any of the three networks.

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
ras> ip ro st
Dest           FF Len Interface  Gateway         Metric stat Timer  Use
192.168.3.0    00 24  enif0:1    192.168.3.1        1    041b 0      0
192.168.2.0    00 24  enif0:0    192.168.2.1        1    041b 0      0
192.168.1.0    00 24  enif0      192.168.1.1        1    041b 0      0
ras>
```

Two new protocol filter interfaces in menu 3.2.1 allow you to accept or deny LAN packets from/to the IP alias 1 and IP alias 2 go through the ZyXEL device. The filter set in menu 3.1 is used for main network configured in menu 3.2.

- IP Alias Setup

1. Edit the first network in menu 3.2 by configuring the ZyXEL device's first LAN IP address.

```
                    Menu 3.2 - TCP/IP and DHCP Ethernet Setup


DHCP= Server                        TCP/IP Setup:
Client IP Pool:
  Starting Address= 192.168.1.33    IP Address= 192.168.1.1
  Size of Client IP Pool= 32        IP Subnet Mask= 255.255.255.0
First DNS Server= From ISP          RIP Direction= Both
  IP Address= N/A                     Version= RIP-1
Second DNS Server= From ISP         Multicast= None
  IP Address= N/A                   Edit IP Alias= Yes
Third DNS Server= From ISP
  IP Address= N/A
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
    DHCP Server Address= N/A

                    Press ENTER to Confirm or ESC to Cancel:
```

Key Settings:

DHCP Setup	If the ZyXEL device's DHCP server is enabled, the IP pool for the clients can be any of the three networks.
TCP/IP Setup	Enter the first LAN IP address for the ZyXEL device. This will create the first route in the enif0 interface.
Edit IP Alias	Toggle to **'Yes'** to enter menu 3.2.1 for setting up the second and third networks.

2. Edit the second and third networks in menu 3.2.1 by configuring the ZyXEL device's second and third LAN IP addresses.

```
                    Menu 3.2.1 - IP Alias Setup
                IP Alias 1= Yes
                  IP Address= 192.168.2.1
                  IP Subnet Mask= 255.255.255.0
                  RIP Direction= None
                  Version= RIP-1
                  Incoming protocol filters=
                  Outgoing protocol filters=
                IP Alias 2= Yes
                  IP Address= 192.168.3.1
                  IP Subnet Mask= 255.255.255.0
                  RIP Direction= None
                  Version= RIP-1
                  Incoming protocol filters=
                  Outgoing protocol filters=

                 Enter here to CONFIRM or ESC to CANCEL:
```

Key Settings:

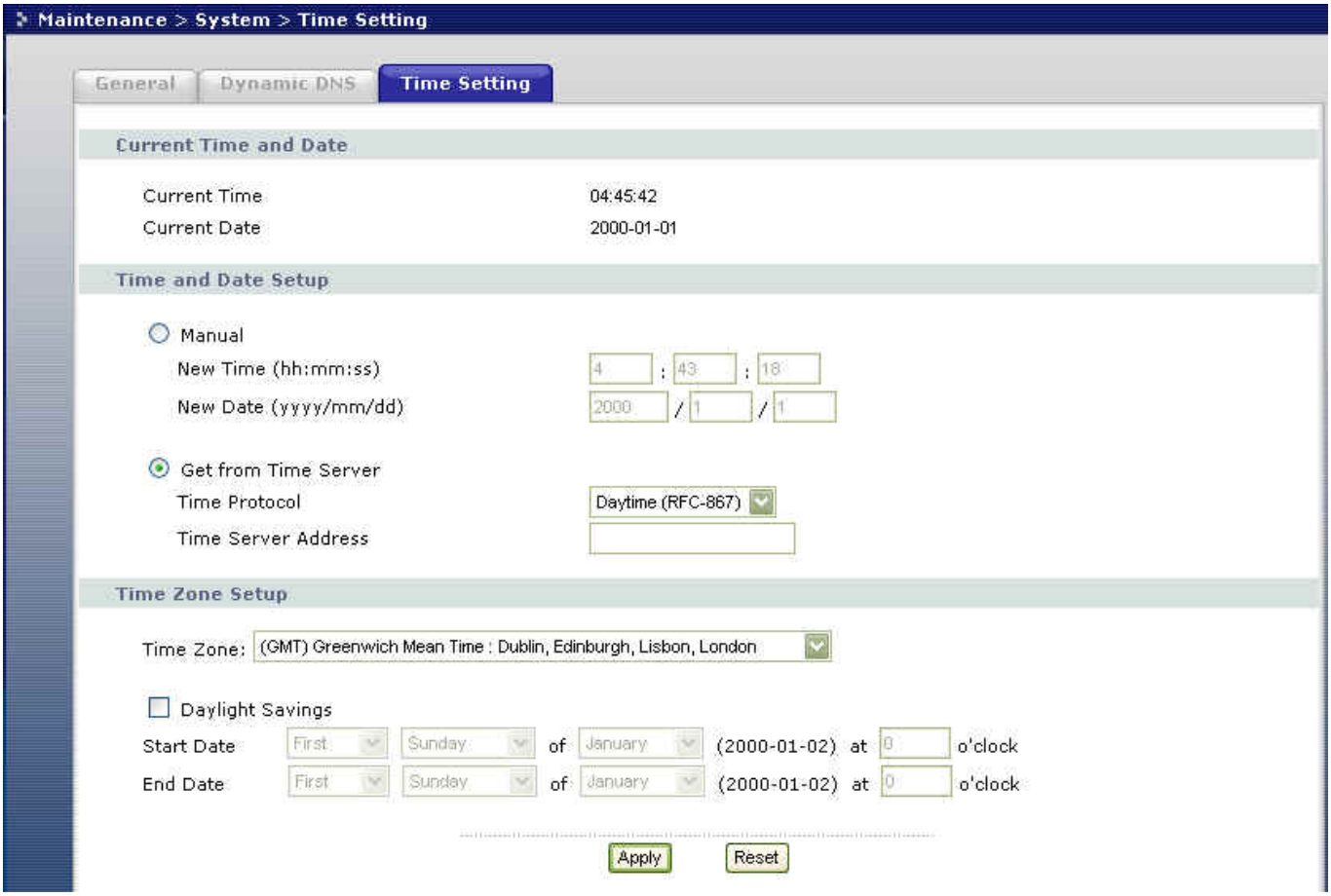
All contents Copyright (c) 2007 ZyXEL Communications Corporation.

IP Alias 1	Toggle to '**Yes**' and enter the second LAN IP address for the ZyXEL device. This will create the second route in the enif0:0 interface.
IP Alias 2	Toggle to '**Yes**' and enter the third LAN IP address for the ZyXEL device. This will create the third route in the enif0:1 interface.

- Time Service in Prestige

There is no RTC (Real-Time Clock) chip so the ZyXEL device should launch a mechanism to get current time and date from external server in boot time. Time service is implemented by the Daytime protocol(RFC-867), Time protocol(RFC-868), and NTP protocol(RFC-1305). You have to assign an IP address of a time server and then, the ZyXEL device will get the date, time, and time-zone information from this server.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.



Using IP Multicast

- What is IP Multicast ?

Traditionally, IP packets are transmitted in two ways - unicast or broadcast. Multicast is a third way to deliver IP packets to a group of hosts. Host groups are identified by class D IP addresses, i.e., those with "1110" as their higher-order bits. In dotted decimal notation, host group addresses range from 224.0.0.0 to 239.255.255.255. Among them, 224.0.0.1 is assigned to the permanent IP hosts group, and 224.0.0.2 is assigned to the multicast routers group.

IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC2236). IP hosts use IGMP to report their multicast group membership to any

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

immediate-neighbor multicast routers so the multicast routers can decide if a multicast packet needs to be forwarded. At start up, the ZyXEL device queries all directly connected networks to gather group membership.

After that, the ZyXEL device updates the information by periodic queries. The ZyXEL device implementation of IGMP is also compatible with version 1. The multicast setting can be turned on or off on Ethernet and remote nodes.

- IP Multicast Setup

Enable IGMP in Prestige's LAN in menu 3.2:

```
                    Menu 3.2 - TCP/IP and DHCP Ethernet Setup

DHCP= Server                        TCP/IP Setup:

Client IP Pool:

  Starting Address= 192.168.1.33    IP Address= 192.168.1.1

  Size of Client IP Pool= 32        IP Subnet Mask= 255.255.255.0

First DNS Server= From ISP          RIP Direction= Both

  IP Address= N/A                     Version= RIP-1

Second DNS Server= From ISP         Multicast= IGMP-v2

  IP Address= N/A                   Edit IP Alias= No

Third DNS Server= From ISP

  IP Address= N/A

DHCP Server Address= N/A

            Press ENTER to Confirm or ESC to Cancel:
```

Enable IGMP in Prestige's remote node in menu 11.3:

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
Menu 11.3 - Remote Node Network Layer Options

  IP Address Assignment= Dynamic
  Rem IP Addr= N/A
  Rem Subnet Mask= N/A
  My WAN Addr= N/A

  Network Address Translation= SUA Only
  Metric= 1
  Private= No
  RIP Direction= Both
    Version= RIP-2B
  Multicast= IGMP-v2

   Enter here to CONFIRM or ESC to CANCEL:
```

Key Settings:

Multicast	IGMP-v1 for IGMP version 1, IGMP-v2 for IGMP version 2.

Using Prestige traffic redirect

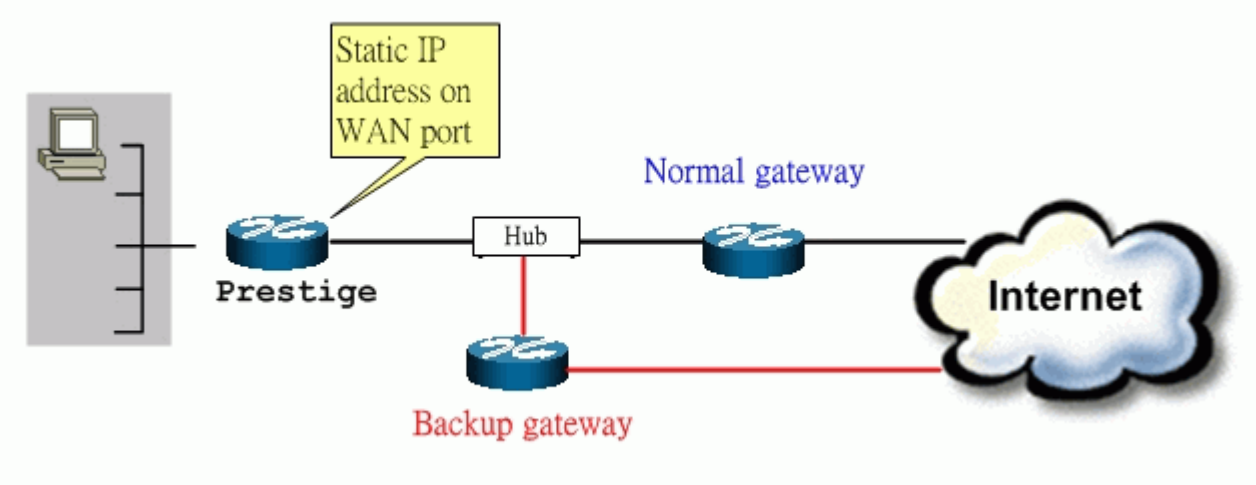
- What is Traffic Redirect ?

Traffic redirect forwards WAN traffic to a backup gateway when Prestige cannot connect to the Internet through it's normal gateway. Thus make your backup gateway as an auxiliary backup of your WAN connection. Once Prestige detects it's WAN connectivity is broken, Prestige will try to forward outgoing traffic to backup gateway that users specify in traffic redirect configuration menu.

- How to deploy backup gateway?

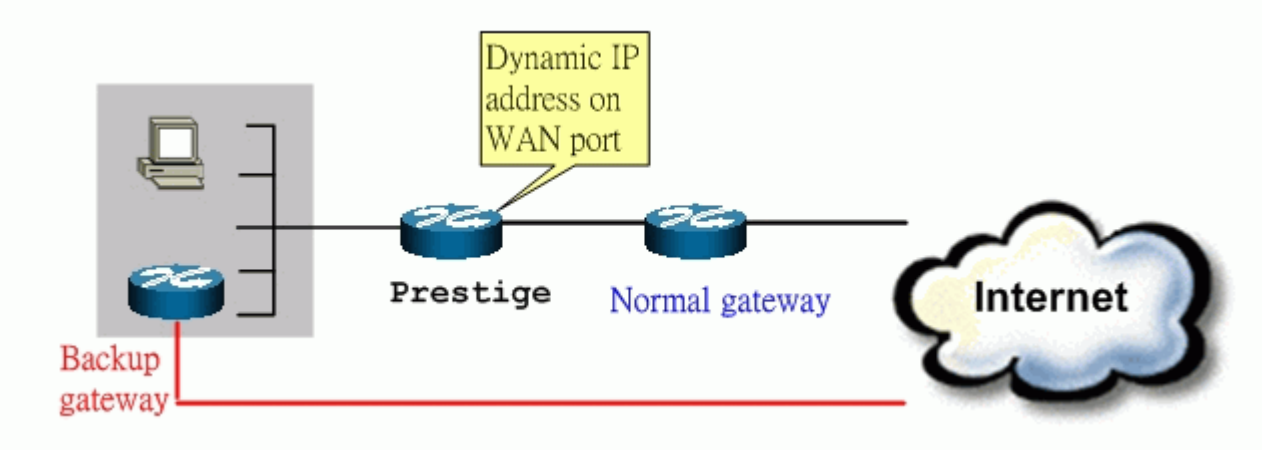
All contents Copyright (c) 2007 ZyXEL Communications Corporation.

You can deploy the backup gateway on the WAN or LAN of Prestige. However, if you would like to deploy the backup gateway on the WAN of Prestige, please make sure that your Prestige has a static WAN IP address at first. Otherwise, we recommend you to deploy the backup gateway on the LAN of Prestige.



Traffic Redirect on WAN port

When Prestige has a dynamic IP address on it's WAN port, it may be easier to connect backup gateway to the LAN of Prestige.



Traffic Redirect on LAN port

- Traffic Redirect Setup

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

Configure parameters that determine when Prestige will forward WAN traffic to the backup gateway using **SMT Menu 11.6-Traffic Redirect Setup.**

```
Menu 11.1 - Remote Node Profile
```

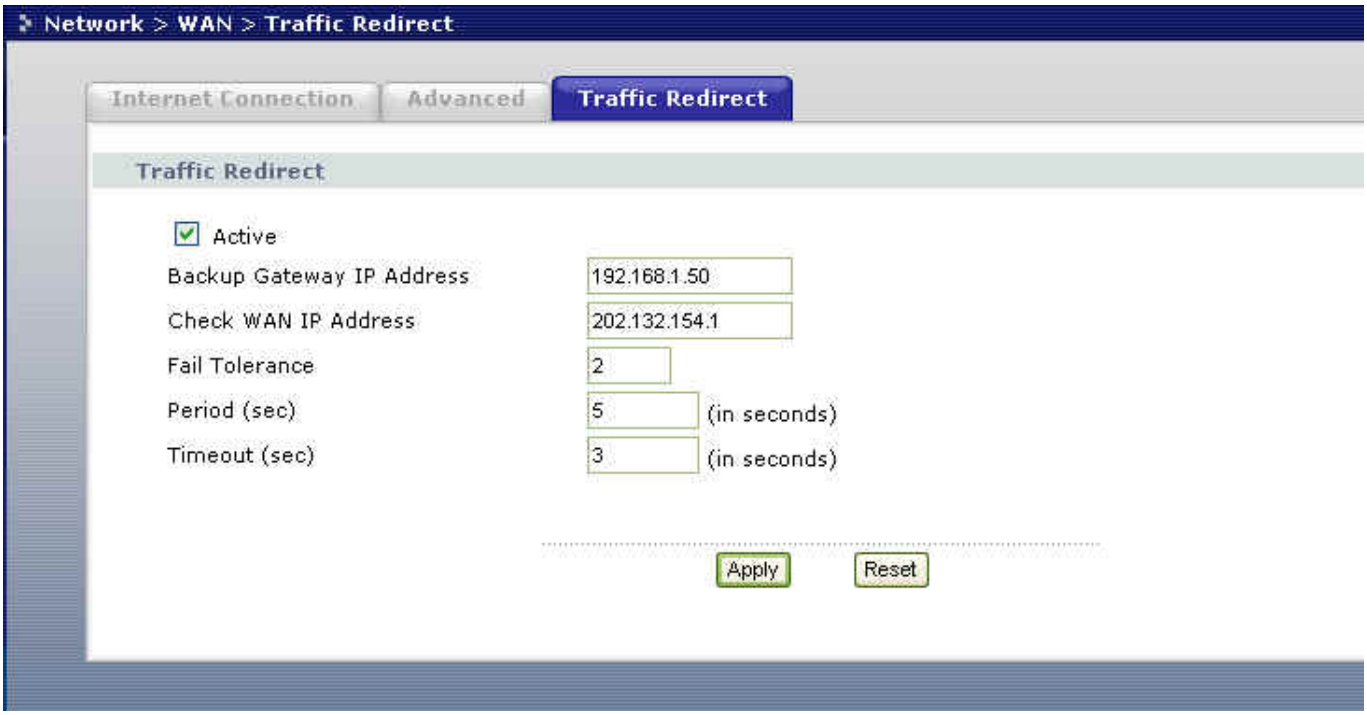
```
                    Menu 11.6 - Traffic Redirect Setup

                Active= Yes
                Configuration:
                  Backup Gateway IP Address= 192.168.1.50
                  Metric= 14
                  Check WAN IP Address= 202.13.154.1
                    Fail Tolerance= 5
                    Period(sec)= 30
                    Timeout(sec)= 3

                Press ENTER to Confirm or ESC to Cancel:
```

Key Settings:

Active	Press [Space BAR] and select **Yes** (to enable) or **No** (to disable) traffic redirect setup.
Backup Gateway IP Address	The IP address of your backup gateway. Prestige automatically forwards outgoing traffic to this IP address if Prestige's Internet connection terminates.
Metric	Enter a number from 1 to 15 to give your traffic redirect route a priority number. The smaller the number, the higher priority the route has.
Check WAN IP Address	Configure a reliable server on Internet (for example, your ISP's DNS server address) for Prestige to check it's WAN connectivity periodically. If you leave this field as 0.0.0.0, Prestige will check it's default gateway IP address instead.
Fail Tolerance	Specify the number of times your Prestige may attempt and fail to connect to Internet before triggering traffic redirect connection.
Period	Specify the period that Prestige would check it's WAN connectivity.
Timeout	Specify the seconds that Prestige would wait for a response from the reliable server.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

You can also configure traffic redirect via web configuration. The configuration page is in ADVANCED/WAN/Traffic Redirect.



Using Universal Plug n Play (UPnP)

- **1. What is UPnP**

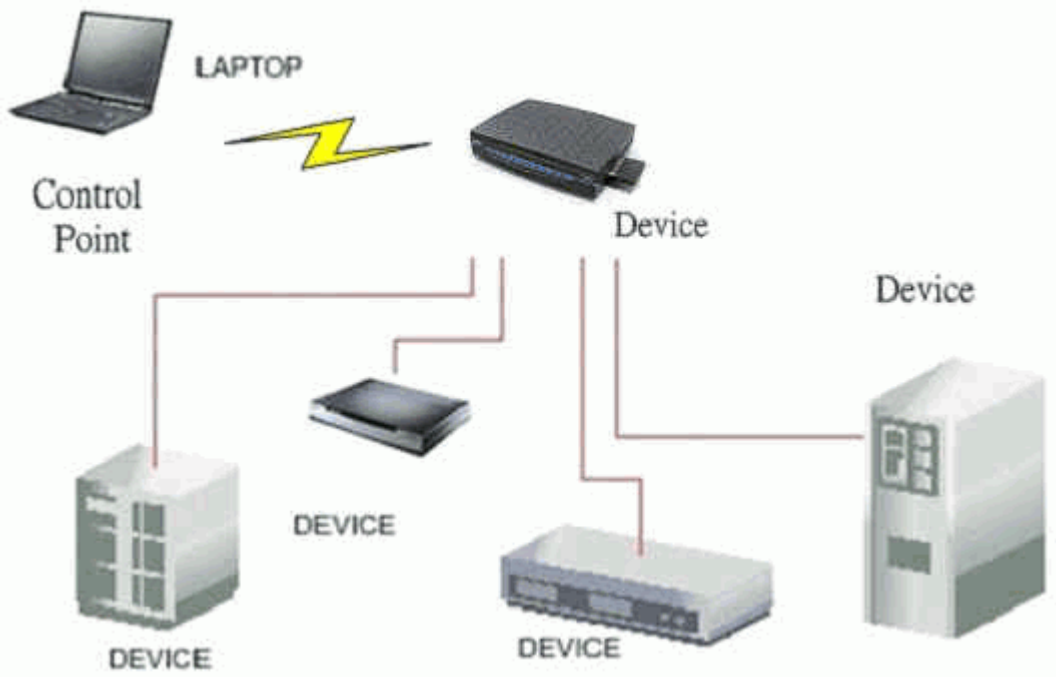
UPnP (Universal Plug and Play) makes connecting PCs of all form factors, intelligent appliances, and wireless devices in the home, office, and everywhere in between easier and even automatic by leveraging TCP/IP and Web technologies. UPnP can be supported on essentially any operating system and works with essentially any type of physical networking media – wired or wireless.

UPnP also supports NAT Traversal which can automatically solve many NAT unfriendly problems. By UPnP, applications assign the dynamic port mappings to Internet gateway and delete the mappings when the connections are complete.

The key components in UPnP are devices, services, and control points.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

- **Devices**: Network devices, such as networking gateways, TV, refrigerators, printers...etc, which provides services.
- **Services**: Services are provided by devices, such as time services provided by alarm clocks. In UPnP, services are described in XML format. Control points can set/get services information from devices.
- **Control points**: Control points can manipulate network devices When you add a new control point (in this case, a laptop) to a network, the device may ask the network to find UPnP-enabled devices. These devices respond with their URLs and device descriptions.



UPnP Operations

- Addressing: UPnPv1 devices MAY support IPv4, IPv6, or both. For IPv4, each devices should have DHCP client, when the device gets connected to the network, it will discover DHCP server on network to get an IP address. If not, then Auto-IP mechanism should be supported so that the device can give itself an IP address.(169.254.0.0/16)
- Discovery: Whenever a device is added on the network, it will advertise it's service over the network. Control point can also discover services provided by devices.
- Description: Control points can get more detailed service information from devices' description in XML format. The description may include product name, model name, serial number, vendor ID, and embedded services...etc.

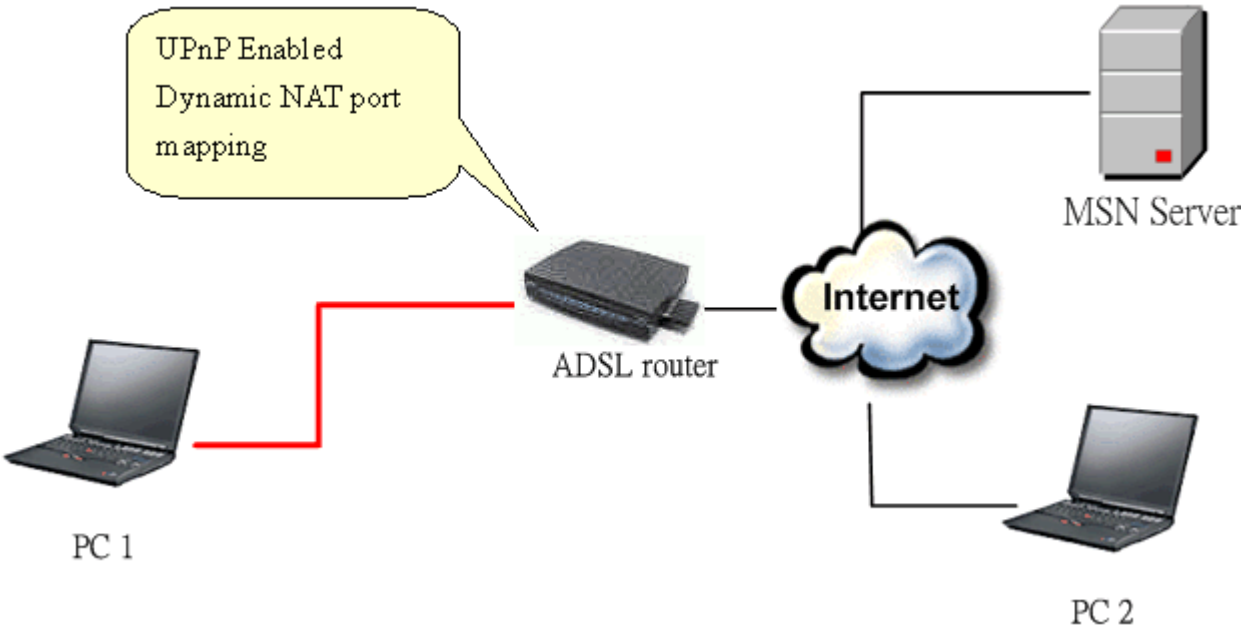
All contents Copyright (c) 2007 ZyXEL Communications Corporation.

- Control: Devices can be manipulated by control points through Control message.
- Eventing: Devices can send event message to notify control points if there is any update on services provided.
- Presentation: Each device can provide their own control interface by URL link. So that users can go to the device's presentation web page by the URL to control this device.

- **2. Using UPnP in ZyXEL devices**

In this example, we will introduce how to enable UPnP function in ZyXEL devices. Currently, Microsoft MSN is the most popular application exploiting UPnP, so we take Microsoft MSN application as an example in this support note. You can learn how MSN benefit from NAT traversal feature in UPnP in this application note.

In the diagram, suppose PC1 and PC2 both sign in MSN server, and they would like to establish a video conference. PC1 is behind PPPoE dial-up router which supports UPnP. Since the router supports UPnP, we don't need to setup NAT mapping for PC1. As long as we enable UPnP function on the router, PC1 will assign the mapping to the router dynamically. Note that since PC1 must support UPnP, we presume that it's OS is Microsoft WinME or WinXP.



Device: Prestige Router
Service: NAT function provided by Prestige Router
Control Point: PC1

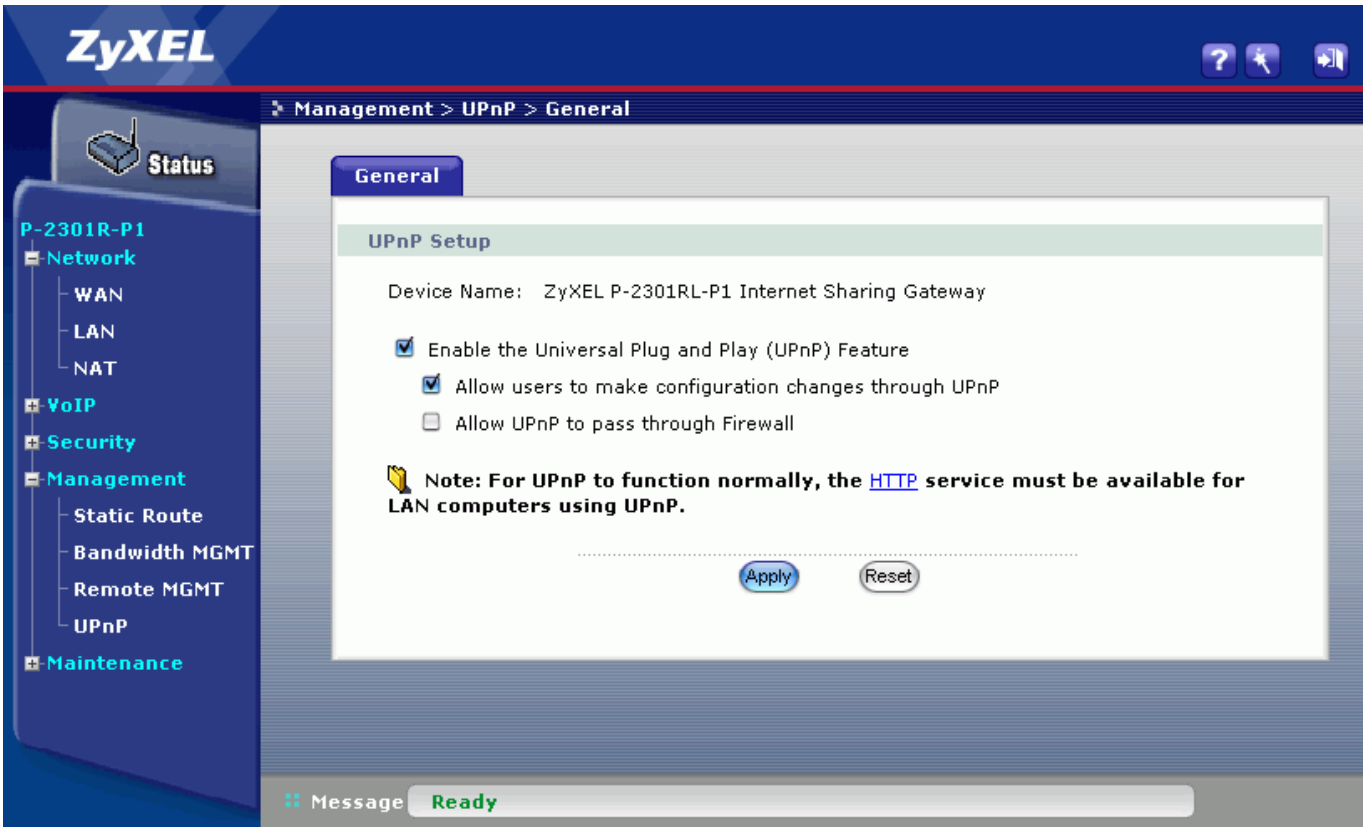
All contents Copyright (c) 2007 ZyXEL Communications Corporation.

1. Enable UPnP function in ZyXEL device

Go to **Management->UPnP**, check two boxes, **Enable UPnP service** and **Allow users to make configuration changes through UPnP.**

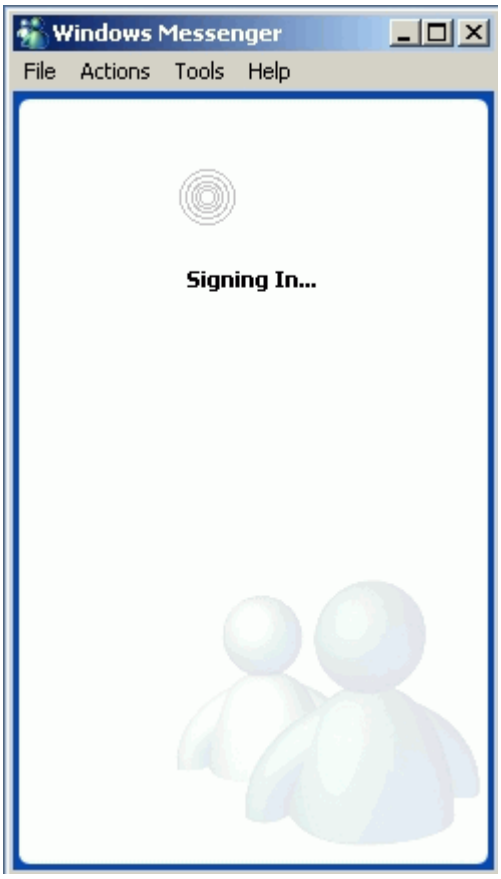
The first check box enables UPnP function in this device.

The second check box allow users' application to change configuration in this device. For instance, if you enable this item, then user's MSN application can assign dynamic port mapping to the router. So that network administrator don't need to setup SUA port mapping in the router.



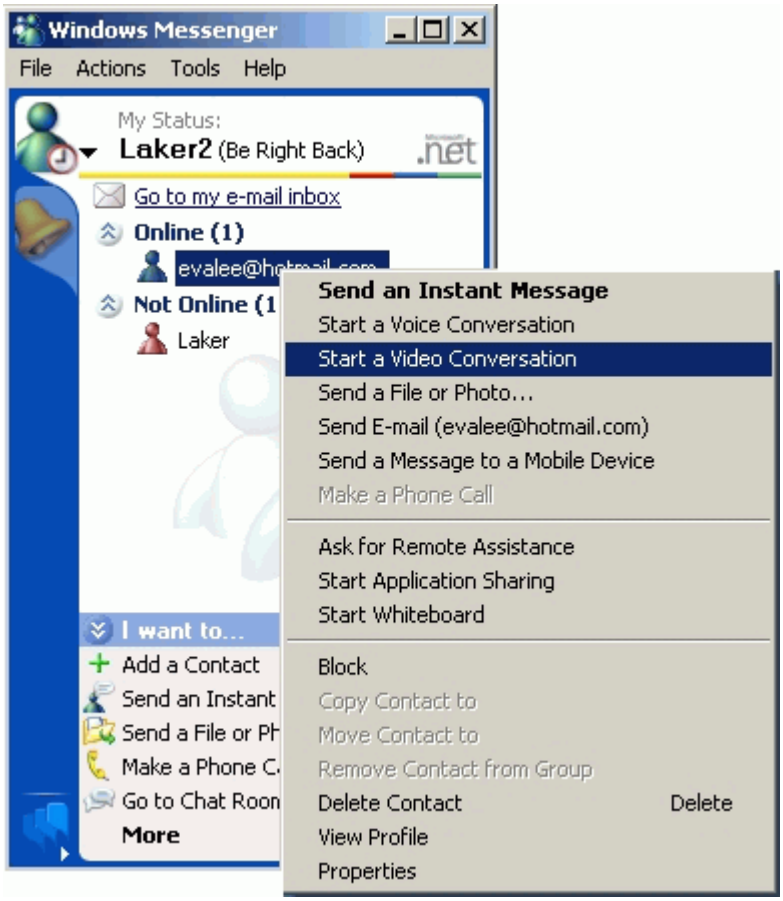
2. After getting IP address, you can go to open MSN application on PC and sign in MSN server.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.



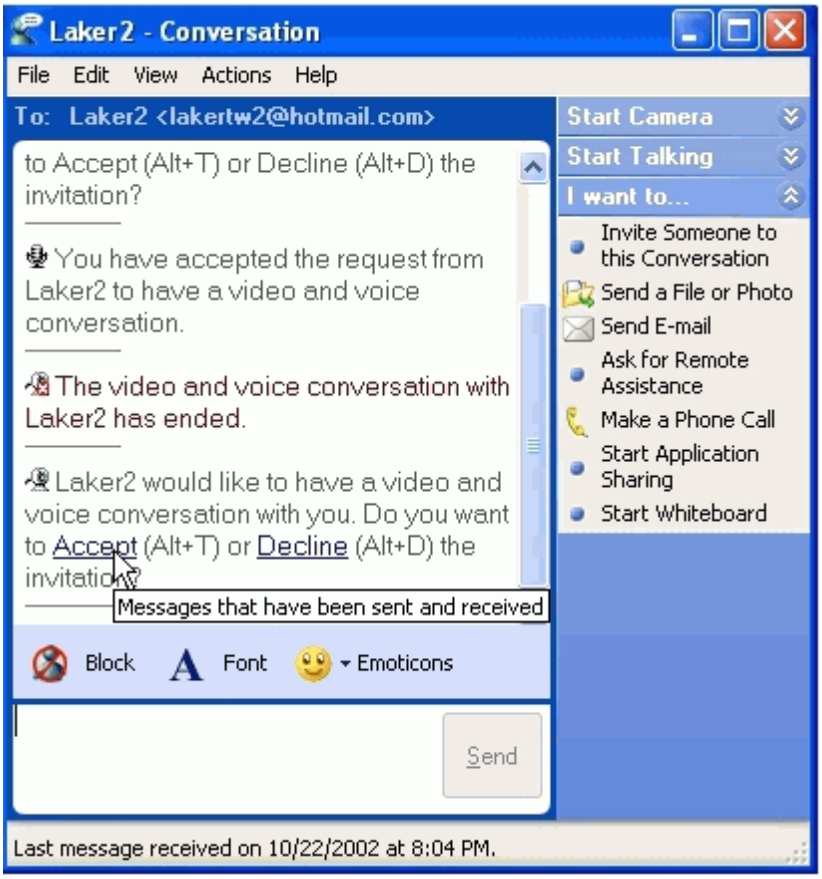
3. Start a Video conversation with one online user.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.



4. On the opposite side, your partner select Accept to accept your conversation request.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.


Laker2 - Conversation
File Edit View Actions Help
To: Laker2 <lakertw2@hotmail.com>
to Accept (Alt+T) or Decline (Alt+D) the invitation?
You have accepted the request from Laker2 to have a video and voice conversation.
The video and voice conversation with Laker2 has ended.
Laker2 would like to have a video and voice conversation with you. Do you want to Accept (Alt+T) or Decline (Alt+D) the invitation?
Messages that have been sent and received
Block
Font
Emoticons
Send
Last message received on 10/22/2002 at 8:04 PM.
Start Camera
Start Talking
I want to...
Invite Someone to this Conversation
Send a File or Photo
Send E-mail
Ask for Remote Assistance
Make a Phone Call
Start Application Sharing
Start Whiteboard

5. Finally, your video conversation is achieved.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

evalee@hotmail.com - Conversation
File Edit View Actions Help
To: evalee@hotmail.com
request to have a video and voice conversation.
The video and voice conversation with evalee@hotmail.com has ended.
You have asked to have a video and voice conversation with evalee@hotmail.com. Please wait for a response or Cancel (Alt+Q) the pending invitation.
evalee@hotmail.com has accepted your request to have a video and voice conversation.
Block
Font
Emoticons
Send
Stop Camera
Options
Stop Talking
Speakers
Microphone
I want to...
Invite Someone to this Conversation
More
Connection established

VoIP Application Notes

Setup SIP Account

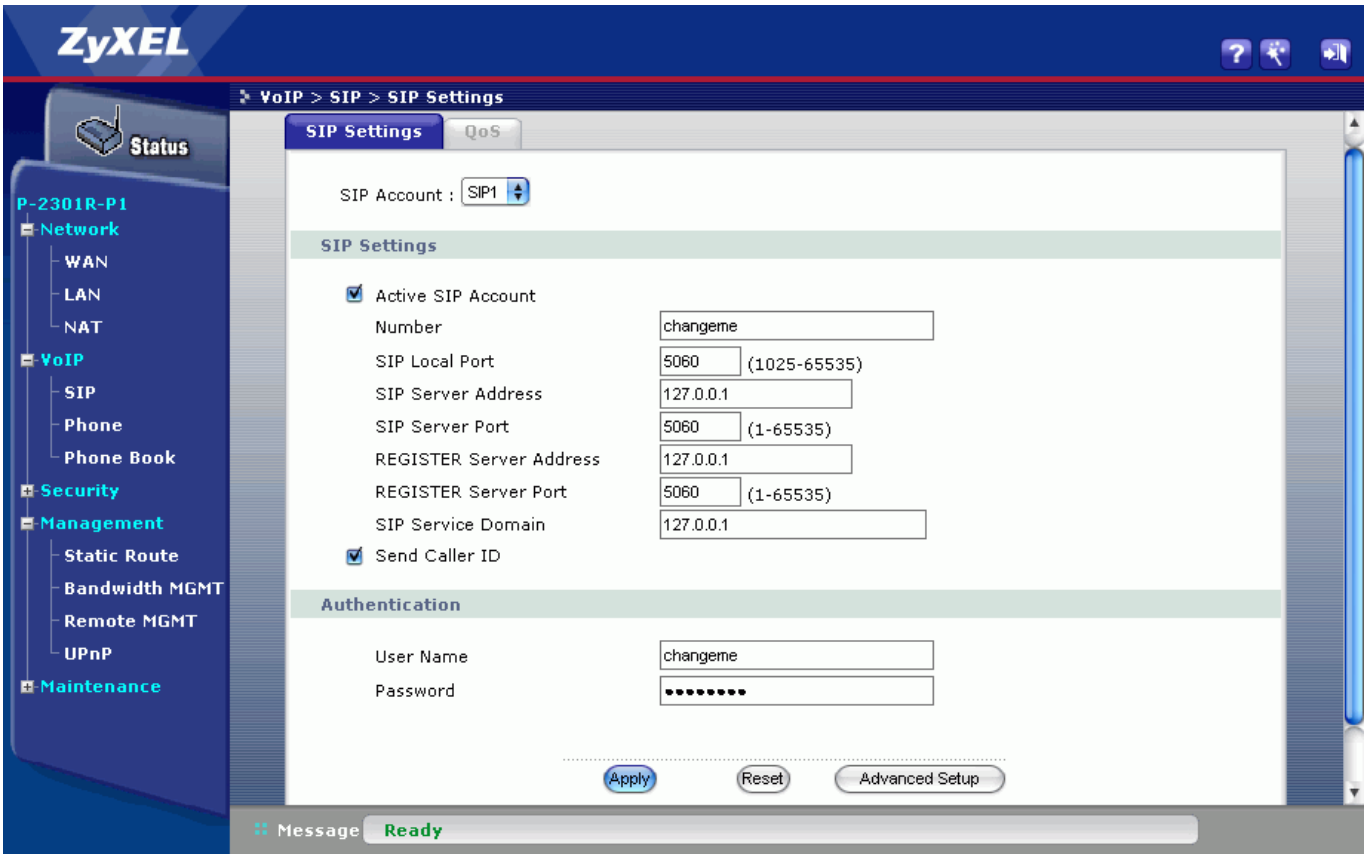
VoIP is the sending of voice signals over the Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network.

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

The ZyXEL device can hold up to two SIP account simultaneously please follow the below instruction to configure the SIP account properly.

Note: You should have a voice account already set up and have VoIP information from your VoIP service provider prior to configure SIP account on to the unit.



With the account information your ITSP provider provided now you may start.

Step 1. Open the web browser from your workstation to connect to the ZyXEL device by entering the Management IP address of the ZyXEL device (LAN IP address). The default management IP of Prestige is 192.168.1.1.

Step 2. Enter the administrator password appear on the page of login and click on login. The default is '1234'

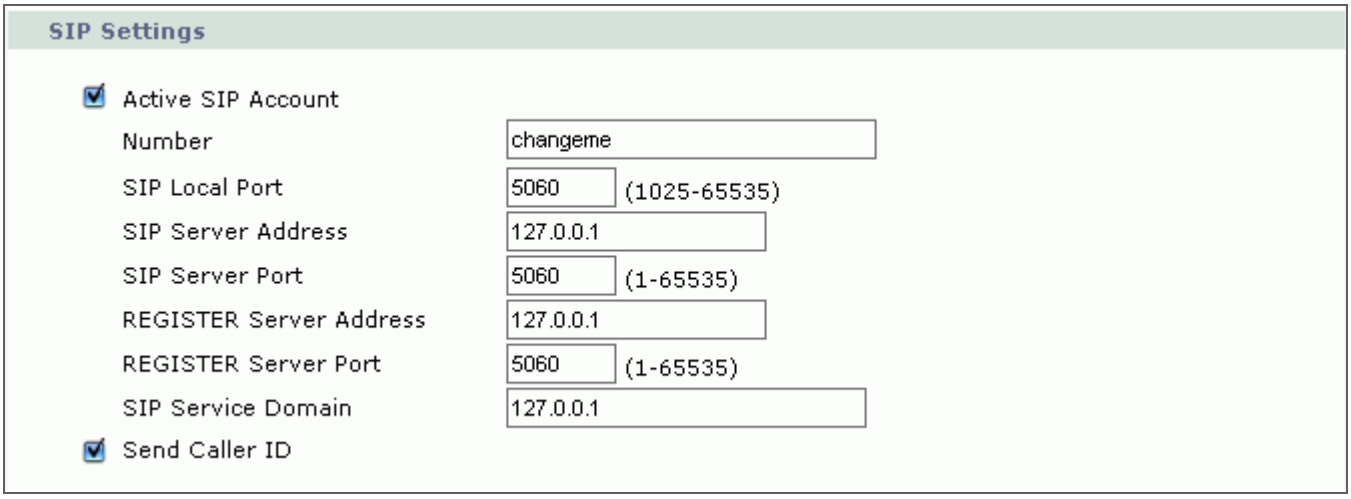
Step 3. On the left column click on Voice to bring you to Voice configuration menu than click on SIP Settings. While in the SIP Settings page use the account selector on upper right of the page to select the SIP account you will like to configure.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

Step 4. Check active box if you like to use this account and fill in the account information the ITSP provided you in the **SIP setting** category. Which will normally include you **SIP number, SIP local port, SIP server address, SIP server port, Register server port, Register server address, SIP service domain.**

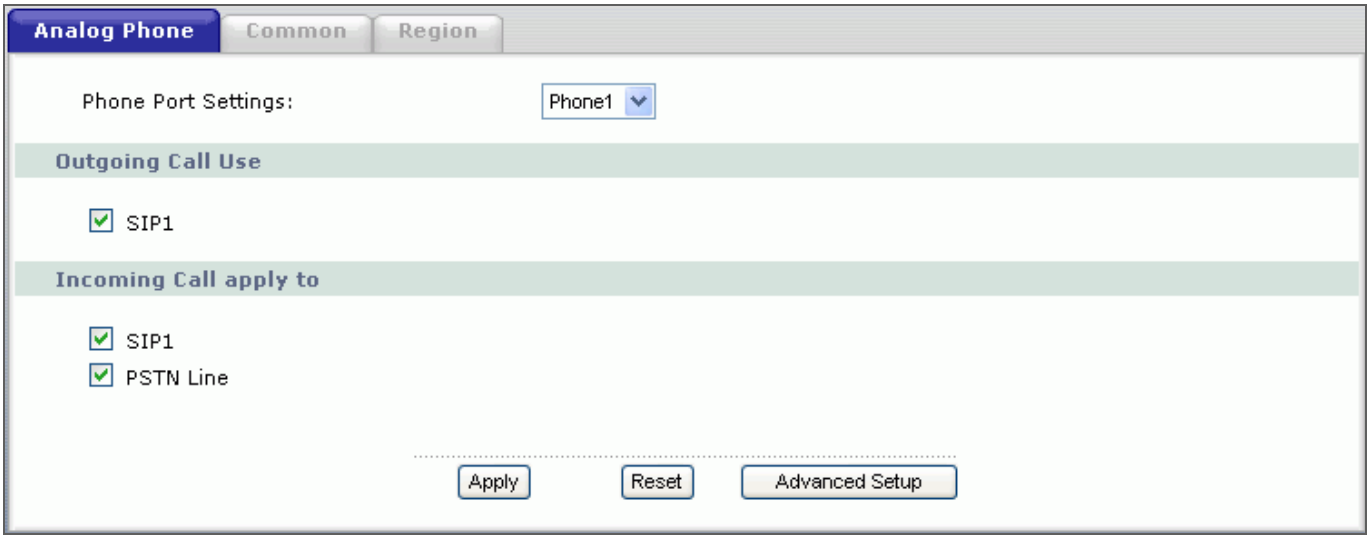
Step 5. In the **Authentication** category fill in the User ID and authentication password your ITSP provided to you.

Step 6. If you wish to send caller ID check the check box in the Caller ID category, if you do not wish to send out caller ID leave the check box uncheck.



Step 7. Check phone port 1 or PSTN Line you will like to associate this account to for incoming call. Prestige allows you to associate one phone port to single SIP account or Lifeline connection. So you can decide whether the analog phone rings when incoming SIP(PSTN) call is received .

All contents Copyright (c) 2007 ZyXEL Communications Corporation.



Step 8. Click on Apply to save the setting and take effect. If you would like to configure the 2nd SIP account, please select SIP2 by using the SIP account selector than follow step 1 to 8 to complete the 2nd account setup.

Note: If more than both SIP number are associated both phone port you will not be able to identify which account is being called for the incoming call.

Each field's detail description on this page is listed below.

Label	Description
SIP Account	You can configure the ZyXEL device to use multiple SIP accounts. Select one to configure its settings on the ZyXEL device.
SIP Number	A SIP account's Uniform Resource Identifier (URI) identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. It is also known as a SIP identity or address. The format of a SIP identity is SIP-Number@SIP-Srevice-Domain. A SIP number is the part of the SIP URI that comes before the "@" symbol. Enter your SIP number in this field. You can use up to 31 ASCII characters.
SIP Local Port	Use this field to configure the ZyXEL device's listening port for SIP. Leave this field set to the default if you were not given a local port number for SIP.
SIP Server	Type the IP address of the SIP server in this field.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

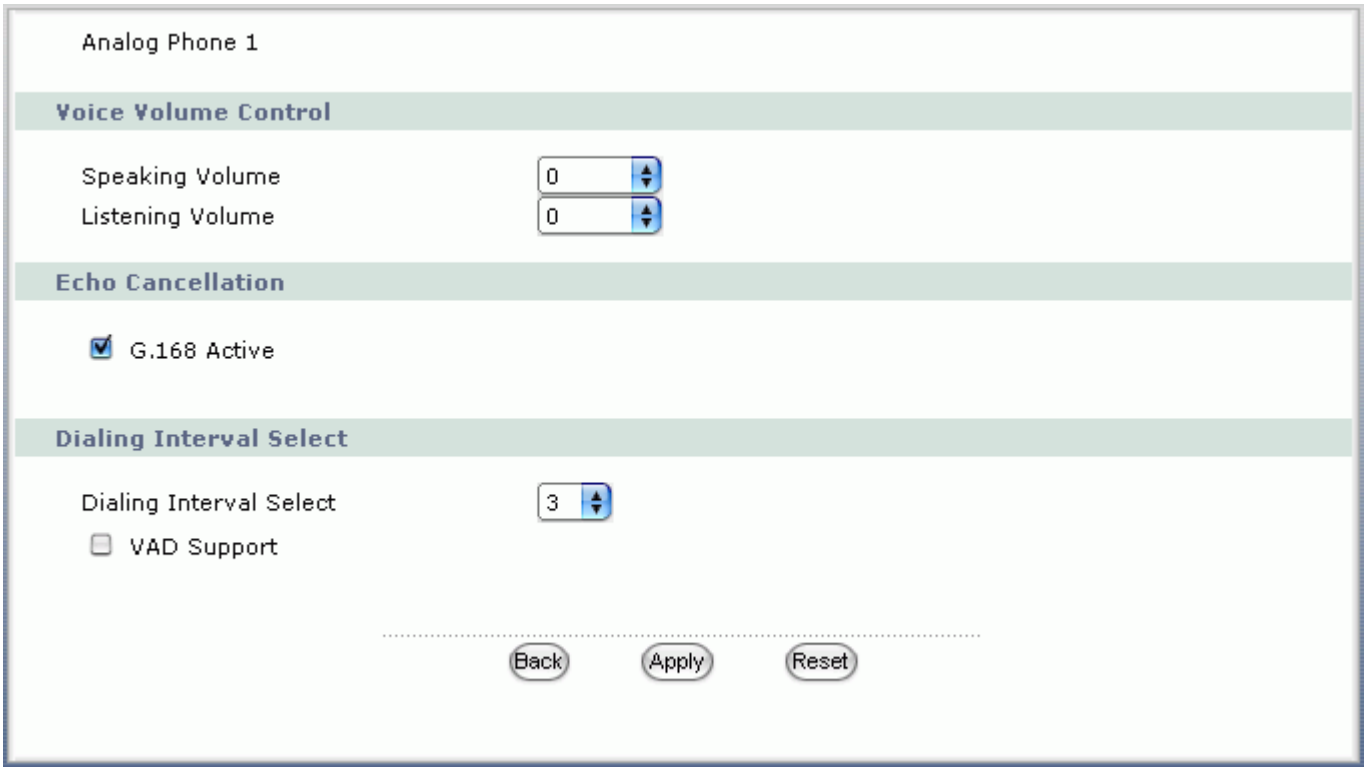
Address	
SIP Server Port	Enter the SIP server's listening port for SIP in this field. Leave this field set to the default if your VoIP service provider did not give you a local port number for SIP.
REGISTER Server Address	A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register. Enter the SIP register server's address in this field. **If you were not given a register server address, then enter the address from the** SIP Server Address **field again here.**
REGISTER Server Port	Enter the SIP register server's listening port for SIP in this field. **If you were not given a register server port, then enter the port from the** SIP Server Port **field again here.**
SIP Service Domain	A SIP service domain is the domain name that comes after the @ symbol in a full SIP URI. Enter the SIP service domain name in this field.You can use up to 127 ASCII Extended set characters.
Authentication User ID	This is the user name for registering this SIP account with the SIP register server. Type the user name exactly as it was given to you. Use ASCII characters.
Authentication Password	Type the password associated with the user name above. Use ASCII Extended set characters.
Block Caller ID	Select this check box to not show identification information when you make VoIP calls. Clear this check box to show identification information when you make VoIP calls.
Apply to	**Phone 1** and **Phone 2** correspond to the ZyXEL device's physical **PHONE 1** and **2** ports, respectively. Select whether you want to receive calls for this SIP account on **Phone 1**, **Phone 2** or both. If you select both, you will not know which SIP account a call is coming in on.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

Advanced Settings	Click **Settings** to open a screen where you can configure the Prestige's advanced VoIP settings like SIP server settings, the RTP port range and the coding type.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

Phone port settings

Prestige allow you to configure the volume and echo cancellation setting for each individual phone port.



To configure the phone port setting please follow the below steps:

Step 1. Open the web browser from your workstation to connect to the Prestige by entering the Management IP address of the Prestige. The default management IP of Prestige is 192.168.1.1.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

Step 2. Enter the administrator password appear on the page of login and click on login. The default is '1234'

Step 3. On the left column click on Voice to bring you to voice function menu. While in the Voice menu click on Phone to enter phone port configuration page.

Step 4. By using the phone port selector located on upper right of the phone port configuration page select the phone port you wish to configure.

Step 5. Change the phone port parameter as you desired and click Apply when you are finish to save and let the setting to take effect. To configure the 2nd phone port use the phone port selector and select phone2 and follow the step 1 to 5 to complete the 2nd phone port setup.

Each field's detail description is listed below.

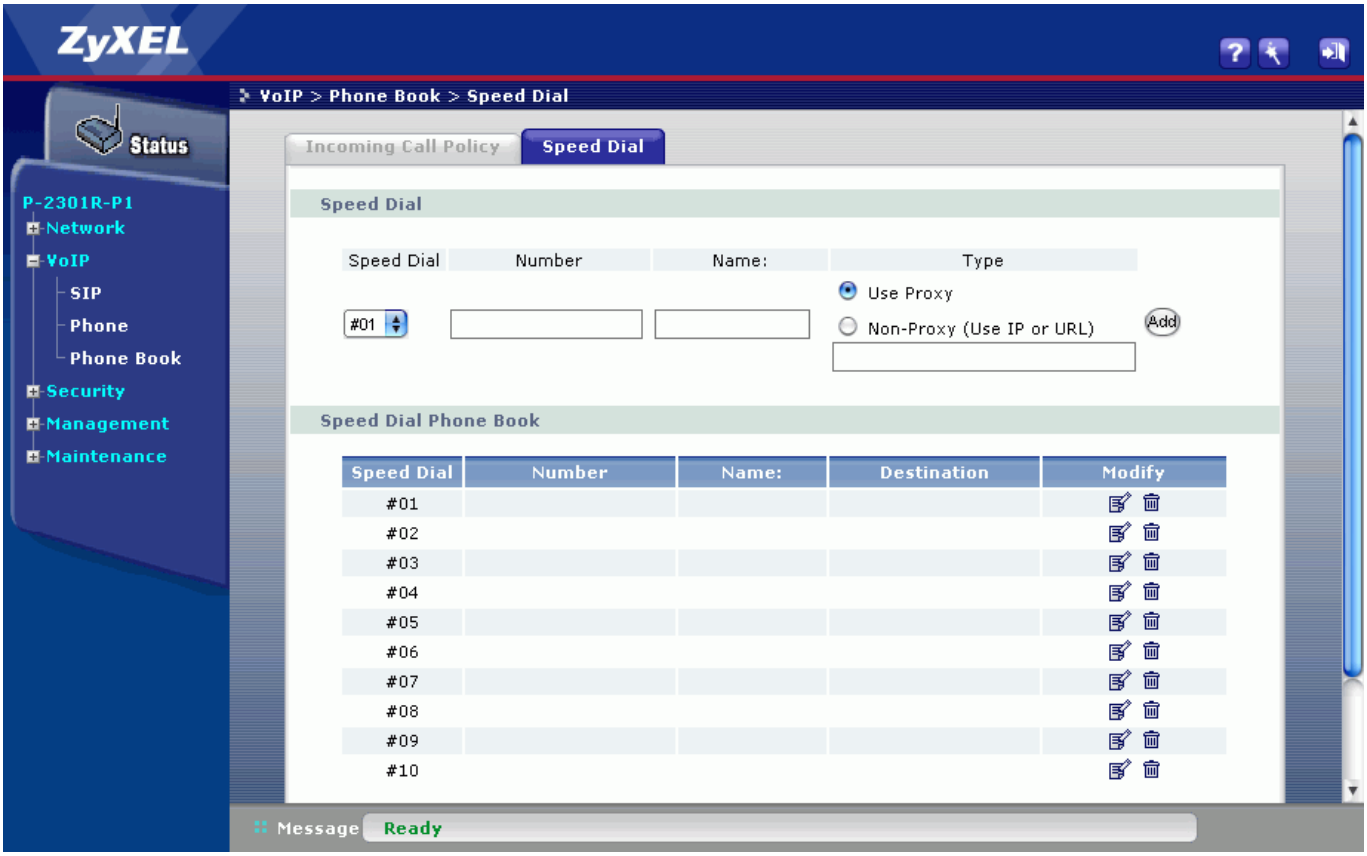
Label	Description
Phone Port Settings	Use this field to select the phone port that you want to configure.
Speaking Volume	Use this field to set the loudness that the Prestige uses for the speech signal that it sends to the peer device. -1 is the quietest and 1 is the loudest.
Listening Volume	Use this field to set the loudness that the Prestige uses for the speech signal that it receives from the peer device and sends to your phone. -1 is the quietest and 1 is the loudest.
Outgoing Call use	**SIP 1** corresponds to the Prestige's SIP account. Select whether you want the phone attached to this phone port to use SIP account 1 when you make a call.
G.168 Active	Select this check box to cancel the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
VAD Support	Select this check box to use Voice Activity Detection (VAD) to reduce the bandwidth that a call uses. The ZyXEL device will generate and send comfort noise when you are not talking.
Dialing Interval	When you are dialing a telephone number the Prestige waits this long after you stop pressing the buttons before initiating the call. Select how many seconds you want the Prestige to wait after the last input on the telephone's keypad before dialing (making) a call.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

Phone book Speed dial

Prestige allows you to configure up to 10 SIP numbers in the phone book for speed dial.



To configure phone book for speed dial please follow the below step.

Step 1. Open the web browser from your workstation to connect to the Prestige by entering the Management IP address of the Prestige. The default management IP of Prestige is 192.168.1.1.

Step 2. Enter the administrator password appear on the page of login and click on login. The default is '1234'

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

Step 3. On the left column click on PHONEBOOK to bring you to Speed Dial page to enter phone book configuration page.

Step 4. Select the entry number you wish to add the to the phone book by the entry selector located under add new entry category on the speed dial field.

Step 5. Fill in the SIP number of the remote party and a descriptive name and click on the radio button to select either to use proxy or entering static IP or URL remote peer.

Step 6. Click on Add button when you are finish to add the entry to the phone book.

Each field's detail description of the page is listed below.

Label	Description
Add New Entry	Use this section of the screen to edit and save new or existing speed dial phone book entries.
Speed Dial	Select a speed dial key combination from the drop-down list box.
SIP Number	Enter the SIP number of the party that you will call (use the number or text that comes before the @ symbol in a full SIP URI). You can use up to 127 ASCII characters.
Name	Enter a descriptive name to identify the party that you will use this entry to call. You can use up to 127 ASCII characters.
Type	Select **Use Proxy** if calls to this party use your SIP account configured in the VoIP screen. Select **Non-Proxy (Use IP or URL)** if calls to this party use a different SIP server or go directly to the callee's VoIP phone (IP-to-IP). Enter the SIP server's or the party's IP address or domain name (up to 127 ASCII Extended set characters).
Add	Click this button to save the entry in the speed dial phone book. The speed dial entry displays in the **Speed Dial Phone Book** section of the screen.
Speed Dial Phone Book	This section of the screen displays the currently saved speed dial entries. You can configure up to 10 entries and use them to make calls.
Speed Dial	This is the entry's speed dial key combination. Press this key combination on

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

	a telephone attached to the Prestige in order to call the party named in this entry.
Name	This is the descriptive name of the party that you will use this speed dial entry to call.
SIP Number	This is the SIP number of the party that you will call.
Type	This field displays **Use Proxy** if calls to this party use one of your SIP accounts. This field displays the SIP server's or the party's IP address or domain name if calls to this party do not use one of your SIP accounts.
Delete	Click this button to remove an entry from the speed dial phonebook.
Edit	Click this button to change the speed dial entry. The speed dial entry displays in the **Add New Entry** section of the screen where you can edit it.
Clear	Click this button to remove all of the entries from the speed dial phonebook.

FAQ

ZyNOS FAQ

What is ZyNOS?

ZyNOS is ZyXEL's proprietary Network Operating System. It is the platform on all Prestige routers that delivers network services and applications. It is designed in a modular fashion so it is easy for developers to add new features. New ZyNOS software upgrades can be easily downloaded from our FTP sites and public Web download site as they become available.

How do I access the embedded web configurator?

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

The Web configurator a user friendly configuration interface via user's web browser, which can be access by typing in the LAN IP address of the Prestige in users web browser. To access the Prestige's web configurator via web browser, the configuration PC must be in the same IP segment of Prestige and Prestige must be reachable to the configuration station. (By default the Prestige LAN IP is 192.168.1.1)

What is the default LAN IP address and Password? Moreover, how do I change it?

The default LAN IP address is "192.168.1.1" and you can change the LAN IP in web configuration menu under "LAN"->LAN TCP/IP, the default password is 1234. You can change the password once you enter the web configuration menu under "SYSTEM" and press the Password tab. At the password screen type in the old password and the new password and retype to confirm than press "Apply" button to save the change.

How do I upload the ZyNOS firmware code via embedded web configurator?

The procedure for uploading ZyNOS via embedded web configurator is as follows.

a. Log on into the web configurator.
b. Press "MAINTENANCE" from the left menu.
c. Press "F/W Upload" tab.
d. Press "browse" button and point to the directory where the firmware you want to upload is kept and press "Upload" button.
e. It will prompt you the firmware is upload successful and Prestige will reboot.

How do I upgrade/backup the ZyNOS firmware by using FTP client program via LAN?

The ZyXEL device allows you to transfer the firmware from/to Prestige by using FTP program via LAN. The procedure for uploading ZyNOS via FTP is as follows.

a. To upgrade firmware, use FTP client program to put firmware in file 'ras' in the Prestige. After data transfer is finished, the Prestige will program the upgraded firmware into FLASH ROM and reboot itself. Note: Do not power off the unit after upload the file via ftp until the system LED have become steady light up. Fail to due so may result in update fail and require RMA.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

b. To backup your firmware, use the FTP client program to get file 'ras' from the Prestige.

How do I upload or backup ROMFILE via web configurator?

In some situations, you may need to upload the ROMFILE, restore to previous saved configuration, orthe need of resetting SMT to factory default.

The procedure for uploading ROMFILE via the web configurator is as follows.

a. Log on into the web configurator.
b. Press "MAINTENANCE" from the left menu.
c. Press "Configuration" tab.
d. Press "Restore" tab and press browse button point to the directory where the romfile you want to upload is stored.
e. Press "Upload" button.

The procedure for backup ROMFILE via the web configurator is as follow

a. Log on into the web configurator.
b. Press "MAINTENANCE" from the left menu.
c. Press "Configuration" tab.
d. Press "Backup" button, a pop up windows will ask you where to store the back up romfile.
e. Press "Save file" and browse to where you want the file be save.
f. Press "Save" button.

How do I backup/restore configurations by using FTP client program via LAN?

a. Use the a FTP client program in your PC (such as cuteftp, wsftp client) to login to your Prestige.
b. To backup the configurations, use FTP client program to get file 'rom-0' from the Prestige.
c. To restore the configurations, use the FTP client program to put your configuration in file ROM-0 in the Prestige.

Why can't I make Telnet to Prestige from WAN?

There are three possible reasons that Telnet from WAN is blocked.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

a. You have not enable Telnet service on WAN interface in Menu 24.11.
b. Telnet service is enabled but your host IP is not the secured host entered in Menu 24.11. In this case, the error message 'Client IP is not allowed!' will appear on the Telnet screen.
c. The default filter rule 3 (Telnet_FTP_WAN) is applied in the Input Protocol field in menu 11.5.

What should I do if I forget the system password?

In case you forget the system password. You can reset the unit back to factory default. You can reset the unit by using a sharp pointed object such as a pen and press and hold down the "reset" button for 5 second or until the power LED starts to blink than release. The unit is than reset back to factory default. The reset button is located near by the power jack on the unit back panel.

Note: By reset the unit back to factory default you will lost all your previous settings.

What is SUA? When should I use SUA?

SUA (Single User Account) is a unique feature supported by Prestige router which allows multiple people to access Internet concurrently for the cost of a single user account.

When Prestige acting as SUA receives a packet from a local client destined for the outside Internet, it replaces the source address in the IP packet header with its own address and the source port in the TCP or UDP header with another value chosen out of a local pool. It then recomputed the appropriate header checksums and forwards the packet to the Internet as if it is originated from Prestige using the IP address assigned by ISP. When reply packets from the external Internet are received by Prestige, the original IP source address and TCP/UDP source port numbers are written into the destination fields of the packet (since it is now moving in the opposite direction), the checksums are recomputed, and the packet is delivered to its true destination. This is because SUA keeps a table of the IP addresses and port numbers of the local systems currently using it.

What is the difference between NAT and SUA?

NAT is a generic name defined in RFC 1631 'The IP Network Address Translator (NAT)'. SUA (Internet Single User Account) is ZyXEL's implementation and trade name for functioning PAT which is a specific type of NAT. SUA (or PAT for NAT) translates address into port mapping.

The primary motivation for RFC 1631 is that there is not enough IP address to go around. In addition, many corporations simply did not bother to obtain legal (globally unique) IP addresses for their networks and now finding themselves unable to connect to the Internet.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

Basically, NAT is a process of translating one address to another. A NAT implementation can be as simple as substituting an IP address with another. This allows a network to rectify the illegal address problem mentioned above without going through each and every host.

The design goal of ZyXEL's SUA is to minimize the Internet access cost in a small office environment by using a single IP address to represent the multiple hosts inside. It does more than IP address translation, so that multiple hosts on the LAN can access the Internet at the same time.

How many network users can the SUA/NAT support?

The ZyXEL device does not limit the number of the users but the number of the sessions. The ZyXEL device supports 1024 sessions that you can use the 'ip nat iface enif0 disp' command in menu 24.8 to view the current active sessions.

What are Device filters and Protocol filters?

In ZyNOS, the filters have been separated into two groups. One group is called 'device filter group', and the other is called 'protocol filter group'. Generic filters belong to the 'device filter group', TCP/IP and IPX filters belong to the 'protocol filter group'.

Why can't I configure device filters or protocol filters?

In ZyNOS, you can not mix different filter groups in the same filter set.

Product FAQ

Is the ZyXEL device an Internet Access Sharing Router?

The ZyXEL device series fulfills a range of application environments, from small and medium businesses, SOHO, or Telecommuters, to home user or education applications. The ZyXEL device series provides a robust Firewall to protect your network, and the IPSec VPN function allows you to create a secure connection for e-business. Prestige's design helps users to save expenses, minimize maintenance, and simultaneously provide a high quality networking environment.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

The ZyXEL device series is a robust solution complete with everything needed for providing Internet access to multiple workstations through your cable or ADSL modem. The router equipped with 2 auto-MDI/MDIX 10/100Mbps Ethernet WAN port, 1 auto-MDI/MDIX 10/100Mbps Ethernet LAN port, 4 auto-MDI/MDIX 10/100Mbps DMZ port and 802.11b wireless capability. It is the most simple and affordable solution for multiple and instant broadband Internet access router with 802.11 wireless support.

Virtually all-popular applications over Internet, such as Web, E-Mail, FTP, Telnet, Gopher, are supported. Prestige is designed for SOHO, branch offices, workgroups, and educational users.

Will the Prestige work with my Internet connection?

The ZyXEL device is designed to be compatible with cable and ADSL modems. Most external Cable and ADSL modems use an Ethernet port to connect to your computer so the Prestige is placed in the line between the computer and the External modem. As long as your Internet Access device has an Ethernet port, you can use the Prestige. Besides, if your ISP supports PPPoE you can also use the Prestige, because PPPoE had been supported in the Prestige.

What do I need to use the Prestige?

You need a ADSL modem or cable modem with an Ethernet port to use the Prestige. The ZyXEL device has two Ethernet ports: LAN port and WAN port. You should connect the computer to the LAN port and connect the external modem to the WAN port. If the ISP uses PPPoE or Roadrunner Authentication you need the user account to enter in the Prestige.

What is PPPoE?

PPPoE stands for Point-to-Point Protocol over Ethernet that is an IETF draft standard specifying how a computer interacts with a broadband modem (i.e. xDSL, cable, wireless, etc.) to achieve access to the high-speed data networks via a familiar PPP dialer such as 'Dial-Up Networking' user interface. PPPoE supports a broad range of existing applications and service including authentication, accounting, secure access and configuration management. There are some service providers running of PPPoE today. Before configuring PPPoE in the Prestige, please make sure your ISP supports PPPoE.

Does the Prestige support PPPoE?

Yes. The ZyXEL device supports PPPoE since ZyNOS 2.50.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

How do I know I am using PPPoE?

PPPoE requires a user account to login to the provider's server. If you need to configure a user name and password on your computer to connect to the ISP you are probably using PPPoE. If you are simply connected to the Internet when you turn on your computer, you probably are not. You can also check your ISP or the information sheet given by the ISP. Please choose PPPoE as the encapsulation type in the Prestige if the ISP uses PPPoE.

Why does my provider use PPPoE?

PPPoE emulates a familiar Dial-Up connection. It allows your ISP to provide services using their existing network configuration over the broadband connections. Besides, PPPoE supports a broad range of existing applications and service including authentication, accounting, secure access and configuration management.

Which Internet Applications can I use with the Prestige?

Most common applications include MIRC, PPTP, ICQ, Cu-SeeMe, NetMeeting, IP/TV, RealPlayer, VDOLive, Quake, QuakeII, QuakeIII, StarCraft, & Quick Time.

How can I configure the Prestige?

a. Telnet remote management- Menu driven user interface for easy remote management
b. Web browser- web server embedded for easy configurations

What network interface does the Prestige support?

The ZyXEL device supports 10/100M Ethernet to connect to the computer and 10/100M Ethernet to connect to the external cable or ADSL modem.

What can we do with Prestige?

Browse the World Wide Web (WWW), send and receive individual e-mail, and download software. These are just a few of many benefits you can enjoy when you put the whole office on-line with the Prestige Internet Access Sharing Router.

Does Prestige support dynamic IP addressing?

The ZyXEL device supports either a static or dynamic IP address from ISP.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

What is the difference between the internal IP and the real IP from my ISP?

Internal IPs is sometimes referred to as virtual IPs. They are a group of up to 255 IPs that are used and recognized internally on the local area network. They are not intended to be recognized on the Internet. The real IP from ISP, instead, can be recognized or pinged by another real IP. The ZyXEL device Internet Access Sharing Router works like an intelligent router that route between the virtual IP and the real IP.

How does e-mail work through the Prestige?

It depends on what kind of IP you have: Static or Dynamic. If your company has a domain name, it means that you have a static IP address. Suppose your company's e-mail address is xxx@mycompany.com. Joe and Debbie will be able to send e-mail through Prestige Internet Access Sharing Router using jane@mycompany.com and debbie@mycompany.com respectively as their e-mail addresses. They will be able to retrieve their individual private and secure e-mail, if they have been assigned the proper access right.

If your company does not have a domain name, it means that your ISP provides you with a dynamic IP address.

Suppose your company's e-mail address is mycompany@ispname.com. Jane and John will be able to send e-mail through Prestige Internet Access Sharing Router using "jane"<mycompany@ispname.com> and "john"<mycompany@ispname.com> respectively as their e-mail addresses. Again, they will be able to retrieve their individual private and secured e-mail, if they have been assigned the proper access right.

What is the difference between the 'Standard' and 'RoadRunner' service?

The US Road Runner service requires the user to "log in" to the service before it can send any packets to the outside network. This is apparently implemented in the TAS (Toshiba Authentication System) with a packet filtering firewall in the upstream direction. Before login, one can send ICMP packets (e.g., ping) to the outside Internet, but nearly all other upstream TCP and UDP packets are blocked. The user can only speak to the local DNS/login server. Downstream packets do not appear to be filtered or blocked at any time.

While Standard service means the cable services which have no login requirement. Prestige supports both Road Runner & Standard services in menu 4 for connecting to cable ISPs.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

Is it possible to access a server running behind SUA from the outside Internet? If possible, how?

Yes, it is possible because Prestige delivers the packet to the local server by looking up to a SUA server table. Therefore, to make a local server accessible to the outside users, the port number and the inside IP address of the server must be configured in Menu 15 - SUA Server Setup.

What DHCP capability does the Prestige support?

The ZyXEL device supports DHCP client on the WAN port and DHCP server on the LAN port. The ZyXEL device's DHCP client allows it to get the Internet IP address from ISP automatically. The ZyXEL device's DHCP server allows it to automatically assign IP and DNS addresses to the clients on the local LAN.

How do I used the reset button, more over what field of parameter will be reset by reset button?

You can used a sharp pointed object insert it into the little reset hole beside the power connector. Press down the reset button and hold down for approx 5 second, the unit will be reset. When the reset button is pressed the devices all parameter will be reset back to factory default include, password, and IP address.

The default IP address is 192.168.1.1, Password 1234.

What network interface does the new Prestige series support?

The new Prestige series support auto MDX/MDIX 10/100M Ethernet LAN/WAN port to connect to the computer on LAN and 10/100M Ethernet to connect to the external cable or ADSL modem on WAN.

How does the Prestige support TFTP?

In addition to the direct console port connection, the Prestige supports the uploading/download of the firmware and configuration file using TFTP (Trivial File Transfer Protocol) over LAN.

Can the Prestige support TFTP over WAN?

Although TFTP should work over WAN as well, it is not recommended because of the potential data corruption problems.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

How can I upload data to outside Internet over the one-way cable?

A workaround is to use an alternate path for your upstream path, such as a dialup connection to an Internet service provider. So, if you can find another way to get your upstream packets to the Internet you will still be able to receive downstream packets via Prestige.

How fast can the data go?

The speed of the cable modem is only one part of the equation. There are a combination of factors starting with how fast your PC can handle IP traffic, then how fast your PC to cable modem interface is, then how fast the cable modem system runs and how much congestion there is on the cable network, then how big a pipe there is at the head end to the rest of the Internet.

Different models of PCs and Macs are able to handle IP traffic at varying speeds. Very few can handle it at 30 Mbps.

Ethernet (10baseT) is the most popular cable modem interface standard for the PC. This automatically limits the speed of the connection to under 10 Mbps even if the cable modem can receive at 30 Mbps. Most Local Area Networks use 10baseT Ethernet, and although they are 10 Mbps networks, it takes a LOT longer than one second to transmit 10 megabits (or 1.25 megabytes) of data from one terminal to another.

Cable modems on the same node share bandwidth, which means that congestion is created when too many people are on simultaneously. One user downloading large graphic or video files can use a significant portion of shared bandwidth, slowing down access for other users in the same neighborhood.

Most independent Internet Service Providers today connect to the Internet using a single 1.5 Mbps "T1" telephone line. All of their subscribers share that 1.5 Mbps pipeline. Cable head-ends connecting to the Internet backbone using a T1 limit their subscribers to an absolute maximum of 1.5 Mbps.

To create the appearance of faster network access, service companies plan to store or "cache" frequently requested web sites and Usenet newsgroups on a server at their head-end. Storing data locally will remove some of the bottleneck at the backbone connection.

How fast can they go? In a perfect world (or lab) they can receive data at speeds up to 30 Mbps. In the real world, with cost conscious cable companies running the systems, the speed will probably fall to about 1.5 Mbps.

My Prestige can not get an IP address from the ISP to connect to the Internet, what can I

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

do?

Currently, there are various ways that ISPs control their users. That is, the WAN IP is provided only when the user is checked as an authorized user. The ISPs currently use three ways:

1. Check if the 'MAC address' is valid
2. Check if the 'Host Name' is valid, e.g., @home
3. Check if the 'User ID' is valid, e.g., RR-Toshiba Authentication Service, RR-Manager Authentication Service

If you are not able to get the Internet IP from the ISP, check which authentication method your ISP uses and troubleshoot the problem as described below.

1. Your ISP checks the 'MAC address'

Some ISPs only provide an IP address to the user with an authorized MAC address. This authorized MAC can be the PC's MAC which is used by the ISP for the authentication. So, if a new network card is used or the Prestige is attached to the cable modem directly, the ISP will reject the DHCP discovery from this MAC, thus no IP is assigned by the ISP.

The ZyXEL device supports to clone the MAC from the first PC the ISP installed to be its WAN MAC. To clone the MAC from the PC you need to enter that PC's IP in menu 2. Once the MAC is received by the Prestige, the WAN MAC in menu 24.1 will be updated and used for the ISP's authentication.

```
MAC Address:
Assigned By= IP address attached on LAN
IP Address= 192.168.1.33
```

Key settings:

a. Assigned By, Choose 'IP address attached on LAN'.
b. IP Address, Enter the IP address of the PC which is installed by the ISP at the first installation.

2. Your ISP checks the 'Host Name'

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

Some ISPs take advantage of the 'host name' message in a DHCP packet such as @home to do the authentication. When first installing, the ISP's tech people configure the host name as the 'Computer Name' of the PC in the 'Networking' settings. When the Prestige is attached to the cable modem to connect to the ISP, we should configure this host name in the Prestige's system (menu 1).

```
Menu 1 - General Setup

System Name= zyxel
```

Key Setting:

- System Name= the system name must be the same as the PC's computer name.

3. Your ISP checks 'User ID'

This authentication type is used by RoadRunner ISP; currently they use RR-TAS (Toshiba Authentication Service) and RR-Manager authentications. You must configure the correct 'Service Type', username and password for your ISP in menu 4.

```
                Menu 4 - Internet Access Setup

          ISP's Name= MyISP
          Encapsulation= Ethernet
            Service Type= RR-Toshiba
            My Login= cso@zyxel
            My Password= ********
            Retype to Confirm= N/A
            Login Server= 0.0.0.0

          IP Address Assignment= Dynamic
            IP Address= N/A
            IP Subnet Mask= N/A
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
                Gateway IP Address= N/A
            Network Address Translation= SUA Only
```

Key settings:

a. Service Type.....Currently, there are two authentication types that Road Runner supports, **RR-TAS** and **RR-Manager.** Choose the correct one for your local ISP.
b. Server IP.....The ZyXEL device will find the Road Runner server IP if this field is blank, otherwise enter the authentication server IP address if you know it.
c. My Login Name...Enter the login name given to you by your ISP
d. My Password.....Enter the password associated with the login name
e. WAN IP Address Assignment...If the ISP did not assign you an explicit IP, select **Dynamic**, otherwise, select **Static**.
f. IP Address & Subnet Mask & Gateway IP Address...Enter the IP address, subnet mask & gateway IP when **Static** Assignment is selected above.

What is BOOTP/DHCP?

BOOTP stands for Bootstrap Protocol. DHCP stands for Dynamic Host Configuration Protocol. Both are mechanisms to dynamically assign an IP address for a TCP/IP client by the server. In this case, the Prestige Internet Access Sharing Router is a BOOTP/DHCP server. Win95 and WinNT clients use DHCP to request an internal IP address, while WFW and WinSock clients use BOOTP. TCP/IP clients may specify their own IP or utilize BOOTP/DHCP to request an IP address.

What is DDNS?

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessed from various locations on the Internet. To use the service, you must first apply an account from several free Web servers such as WWW.DYNDNS.ORG.

Without DDNS, we always tell the users to use the WAN IP of the 312 to reach our internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported by the Prestige, you apply a DNS name (e.g., www.zyxel.com.tw) for your server (e.g., Web server) from a DDNS server. The outside users can always access the web server using the www.zyxel.com.tw regardless of the WAN IP of the 312.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

When the ISP assigns the Prestige a new IP, the Prestige updates this IP to DDNS server so that the server can update its IP-to-DNS entry. Once the IP-to-DNS table in the DDNS server is updated, the DNS name for your web server (i.e., www.zyxel.com.tw) is still usable.

When do I need DDNS service?

When you want your internal server to be accessed by using DNS name rather than using the dynamic IP address we can use the DDNS service. The DDNS server allows to alias a dynamic IP address to a static hostname. Whenever the ISP assigns you a new IP, the Prestige sends this IP to the DDNS server for its updates.

What DDNS servers does the Prestige support?

The DDNS servers the Prestige supports currently is WWW.DYNDNS.ORG where you apply the DNS from and update the WAN IP to.

What is DDNS wildcard?

Some DDNS servers support the wildcard feature which allows the hostname, *.yourhost.dyndns.org, to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful when there are multiple servers inside and you want users to be able to use things such as www.yourhost.dyndns.org and still reach your hostname.

Does the Prestige support DDNS wildcard?

Yes, the Prestige supports DDNS wildcard that WWW.DynDNS.ORG supports. When using wildcard, you simply enter yourhost.dyndns.org in the Host field in Menu 1.1.

Can the Prestige SUA handle IPsec packets sent by the VPN gateway behind Prestige?

Yes, the Prestige's SUA can handle IPsec ESP Tunneling mode. We know when packets go through SUA, SUA will change the source IP address and source port for the host. To pass IPsec packets, SUA must understand the ESP packet with protocol number 50, replace the source IP address of the IPsec gateway to the router's WAN IP address. However, SUA should not change the source port of the UDP packets which are used for key managements. Because the remote gateway checks this source port during connections, the port thus is not allowed to be changed.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

How do I setup my Prestige for routing IPsec packets over SUA?

For outgoing IPsec tunnels, no extra setting is required. For forwarding the inbound IPsec ESP tunnel, A 'Default' server set in menu 15 is required. It is because SUA makes your LAN appear as a single machine to the outside world. LAN users are invisible to outside users. So, to make an internal server for outside access, we must specify the service port and the LAN IP of this server in Menu 15. Thus SUA is able to forward the incoming packets to the requested service behind SUA and the outside users access the server using the Prestige's WAN IP address. So, we have to configure the internal IPsec as a default server (unspecified service port) in menu 15 when it acts a server gateway.

VoIP FAQ

What is Voice over IP?

Voice over IP is an emerging technology based on open standards of IEEE, fundamentally the Internet Protocol, that allows voice data to travel across the Internet. There are many method to used this technology, the most common and well known are SIP, and H.323.

How does Voice over IP work?

Basically VoIP is a technic to send voice information in digital form in discrete packets over digital network rather than by using traditional circuit switch (PSTN). To do so we will need an analog to digital converter on sender side to translate the voice (analog signal) to digital than transmit it, and on the receiver end it will also need an analog to digital converter to covert the digital signal back to analog to the person being called can heard the voice.

Why use VoIP?

Traditionally telephony carrier use circuit switching for carrying voice traffic. As circuit switching is designed to carry voice and it does it very well. Than why use IP for voice? As broadband booms, and technology evolve. People now want to communicate through various way not just voice such as email, instant messaging, video and so on. Traditional telephony can not evolve as quickly as the demand and develop new feature on circuit switch takes much time and money. IP is an already exist standard and many type of service already runs on IP, by using IP as a platform integrate service is now possible and low cost where traditional circuit may take long time to achieve.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

What is the relationship between codec and VoIP?

In order to transfer voice (analog signal) over IP it first need to be digitized. Codec is a technic to digitize analog signal to digital and vice versa. There are various speech codec available and can be used with VoIP each with it's advantage and disadvantage.

What advantage does Voice over IP can provide?

The advantage of VoIP is it can provide advance services such as joining e-mail, instant messaging, video, voice mail all together. Where current circuit switching (PSTN) can not.

What is the difference between H.323 and SIP?

H.323 and SIP are proposed by different group Session Initiation Protocol (SIP) is a standard introduced by the Internet Engineering Task Force in 1999 to carry voice over IP. Since it was created by the IETF, it approaches voice and multimedia from the Internet, or IP, perspective of view. Where as H.323 emerged around 1996, and as an International Telecommunication Union standard it was designed from a telecommunications perspective. Both standards have the same objective - to enable voice and multimedia convergence with IP protocols.

Can H.323 and SIP interoperate with one another?

In interoperability between the two, the industry is making slow but sure progress. Interoperability must first happen between vendor implementations of the same protocol (SIP-to-SIP and H.323-to-H.323) and then between protocols. Currently in order for SIP client to talk to H.323 client the ITSP must have a trunking gateway act as a translator between the two protocols without the truncking gateway the two protocols are not able to communicate to one another.

What is voice quality?

Voice quality is how well an person can hear the voice on the opposite end.

How are voice quality normally rated?

Voice quality is most commonly rated through a voice quality metric called the Mean Opinion Score (MOS) which is recommendation by ITU-T. The MOS is a 5 point scale where 5 represent excellent voice quality and 1 represent bad voice quality.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

What is codec?

Codec is a algorithm which converts analog signal into digital signal and vice versa. There are three main type of waveform codec, source codec, and hybrid codec. Each consume different amount of bandwidth and provide different voice quality level.

What is the relation of codec and VoIP?

As VoIP is a general term send voice information in digital form in discrete packets over digital network and this digital network is public network, thus there maybe other packet such data packet uses network at the same time. The codec choose is related to how much bandwidth voice packet will consume. In bandwidthwise aspect the smaller amount of bandwidth used the better. But in voice aspect the higher quality the better.

What codec does Prestige support?

Prestige supports the following commonly used codec.

- G.729 voice codec
- G.711u-law voice codec
- G.711a-law voice codec

Which codec should I choose?

As which codec choose is depending on what codec is supported on both end of the VoIP host. Generally a codec with low bandwidth consumption and high voice quality is a good codec .

What do I need in order to use SIP?

The minimum required to use VoIP is as follow.

1. A high-speed Internet connection. This can be a cable modem, or a high-speed network services such as ISDN, DSL or a T-1 link. The need of the bandwidth required will depend on the amount of telephone traffic will be in your network.

2. A PC with VoIP software installed or a hardware VoIP box such as ATA or device like Prestige 2302 VoIP station router.

3. An account with a VoIP provider such as an ITSP. The account can be configured to recognize your calls automatically, or you can require the users to enter their unique account numbers issued.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

Unable to register with the SIP server?

If you are unable to register with SIP server.

1. Make sure the Internet is reachable and the SIP register server is reachable. If your register server uses domain name make sure DNS name can be resolved. If you are using static WAN IP make sure DNS server is configured correctly on your Prestige.

2. Make sure the SIP account is correct and the password is key in correctly.

3. Check if there is NAT router before it. Prestige is a VoIP station gateway. We do not suggest to have an NAT router before it as it may cause many unexpected problem. If you have an NAT router before it we suggest to use a VoIP ATA (VoIP Analog Telephone Adapter) such as Prestige ATA series.

I can register but can not establish a call?

If you can register to server but can not make a call very likely there is NAT router or firewall before it which is blocking it. We do not suggest to have an NAT router before it as it may cause many unexpected problem. If you have an NAT router before it we suggest to use a VoIP ATA (VoIP Analog Telephone Adapter) such as Prestige ATA series.

If the problem is a firewall before it. Please check with the firewall manager, make sure the SIP protocol is allow to pass-through firewall, and the range of RTP port is allowed through firewall.

I can make a call but the voice only goes one way not bothway?

If you can register to server and I can make a call signal establishment but the voice only goes one way. In this case it is very likely there are NAT router or firewall before it, please see NAT/firewall related question above.

I can receive a call but the voice only goes one way not bothway?

If you can register to server but can only make out going call but can not receive incoming calls or the incoming call signal establishment can be made but voice only goes one way very likely there is NAT/firewall router before it, please see NAT/firewall related question above for tips to troubleshoot.

If all the about have been tried, but register still fail what should I do?

In such case, please contact your local vendor for support. If they can't help out the problem they will escalate your problem to ZyXEL tech center. To report a problem please prepared below info.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

1. Serial number of the device.

2. SIP Call server type and vendor.

3. Your device firmware version and romfile with password.

4. Detail information what you have tried to resolve the problem.

I suspect there is a hardware problem with my Prestige what should I do?

Please follow the troubleshooting section in the user's guide for brief hardware troubleshooting and diagnostic tips. If you are sure there is a hardware problem after following the hardware diagnostic tips in the user's guide. Please contact your ZyXEL local vendor to send the device in for RMA service.

Trouble Shooting

Unable to Get WAN IP from ISP

My Prestige can not get an IP address from the ISP to connect to the Internet, what can I do?

Currently, there are various ways that ISPs control their users. That is, the WAN IP is provided only when the user is checked as an authorized user. The ISPs currently use three ways:

1. Check if the 'MAC address' is valid
2. Check if the 'Host Name' is valid, e.g., @home
3. Check if the 'User ID' is valid, e.g., RR-Toshiba Authentication Service, RR-Manager Authentication Service

If you are not able to get the Internet IP from the ISP, check which authentication method your ISP uses and troubleshoot the problem as described below.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

1. Your ISP checks the 'MAC address'

Some ISPs only provide an IP address to the user with an authorized MAC address. This authorized MAC can be the PC's MAC which is used by the ISP for authentication. So, if a new network card is used or the Prestige is attached to the cable modem directly, the ISP will reject the DHCP discovery from this MAC, thus no IP is assigned by the ISP.

The problem can be simply solved if the ISP allows you to use a new MAC, and you just tell them the WAN MAC of the Prestige. The WAN MAC of the Prestige can be obtained from menu 24.1.

In case the ISP does not allow you to use a new MAC, the Prestige can clone the MAC from the first PC you installed as the WAN MAC and send it to the ISP. To clone the MAC from the PC you need to enter that PC's IP in menu 2. Once the MAC is received by the Prestige, the WAN MAC in menu 24.1 will be updated.

```
                    Menu 2 - WAN Setup

               MAC Address:

                 Assigned By= IP address attached on LAN

                 IP Address= 192.168.1.33
```

Key settings:

- Assigned By=, Choose **'IP address attached on LAN'**.
- IP Address=, Enter the IP address of the PC which is installed by the ISP at the first installation.

---

2. Your ISP checks the 'Host Name'

Some ISPs take advantage of the 'host name' message in a DHCP packet such as @home to do the authentication. When first installing, the ISP's tech people configure the host name as the 'Computer

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

Name' of the PC in the 'Networking' settings. When the Prestige is attached to the cable modem to connect to the ISP, we should configure this host name in the Prestige's system (menu 1).

```
                Menu 1 - General Setup

System Name= zyxel

Domain Name=

First System DNS Server= From ISP

  IP Address= N/A

Second System DNS Server= From ISP

  IP Address= N/A

Third System DNS Server= From ISP

  IP Address= N/A

Edit Dynamic DNS= No
```

Key Setting:

- System Name=, The system name must be the same as the PC's computer name.

---

3. Your ISP checks 'User ID'

This authentication type is used by RoadRunner ISP, currently they use RR-TAS(Toshiba Authentication Service) and RR-Manager authentications. You must configure the correct 'Service Type', username and password for your ISP in menu 4.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
                Menu 4 - Internet Access Setup

        ISP's Name= MyISP

        Encapsulation= Ethernet

          Service Type= RR-Toshiba

          My Login= cso@zyxel

          My Password= ********

          Retype to Confirm= N/A

          Login Server= 0.0.0.0

        IP Address Assignment= Dynamic

          IP Address= N/A

          IP Subnet Mask= N/A

          Gateway IP Address= N/A

        Network Address Translation= SUA Only
```

Key settings:

- Service Type.....Currently, there are two authentication types that Road Runner supports, **RR-TAS** and **RR-Manager.** Choose the correct one for your local ISP.
- Server IP.....The ZyXEL device will find the Road Runner server IP if this field is blank, otherwise enter the authentication server IP address if you know it.
- My Login Name...Enter the login name given to you by your ISP
- My Password.....Enter the password associated with the login name
- WAN IP Address Assignment...If the ISP did not assign you an explicit IP, select **Dynamic**, otherwise, select **Static**.
- IP Address & Subnet Mask & Gateway IP Address...Enter the IP address, subnet mask & gateway IP when **Static** Assignment is selected above.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

Using Embedded Packet Trace

Embedded Packet Trace

The ZyXEL device packet trace records and analyzes packets running on LAN and WAN interfaces. It is designed for users with technical backgrounds who are interested in the details of the packet flow on LAN or WAN end of Prestige. It is also very helpful for diagnostics if you have compatibility problems with your ISP or if you want to know the details of a packet for configuring a filter rule.

The format of the display is as following:

Packet:

```
0     11880.160 ENET0-R[0062] TCP 192.168.1.2:1108->192.31.7.130:80
```

[index] [timer/second][channel-receive/transmit][length] [protocol] [sourceIP/port] [destIP/port]

There are two ways to dump the trace:

1. **Online Trace--display the trace real time on screen**
2. **Offline Trace--capture the trace first and display later**

The details for capturing the trace in SMT menu 24.8 are as follows.

Online Trace

1. Trace LAN packet
2. Trace WAN packet

---

1. Trace LAN packet

1.1 Disable to capture the WAN packet by entering: `sys trcp channel enet1 none`
1.2 Enable to capture the LAN packet by entering: `sys trcp channel enet0 bothway`
1.3 Enable the trace log by entering: `sys trcp sw on` & **`sys trcl sw on`**
1.4 Display the brief trace online by entering: `sys trcd brief`

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

or

1.5 Display the detailed trace online by entering: sys trcd parse

Example:

```
Prestige> sys trcp channel enet1 none
Prestige> sys trcp channel enet0 bothway
Prestige> sys trcp sw on
Prestige> sys trcl sw on
Prestige> sys trcd brief
   0    11880.160 ENET0-R[0062] TCP 192.168.1.2:1108->192.31.7.130:80
   1    11883.100 ENET0-R[0062] TCP 192.168.1.2:1108->192.31.7.130:80
   2    11883.330 ENET0-T[0058] TCP 192.31.7.130:80->192.168.1.2:1108
   3    11883.340 ENET0-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
   4    11883.340 ENET0-R[0339] TCP 192.168.1.2:1108->192.31.7.130:80
   5    11883.610 ENET0-T[0054] TCP 192.31.7.130:80->192.168.1.2:1108
   6    11883.620 ENET0-T[0102] TCP 192.31.7.130:80->192.168.1.2:1108
   7    11883.630 ENET0-T[0054] TCP 192.31.7.130:80->192.168.1.2:1108
   8    11883.630 ENET0-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
   9    11883.650 ENET0-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
  10    11883.650 ENET0-R[0062] TCP 192.168.1.2:1109->192.31.7.130:80
Prestige> sys trcd parse
---<0000>--------------------------------------------------------------
LAN Frame: ENET0-RECV   Size:  62/  62   Time: 12089.790 sec
Frame Type: TCP 192.168.1.2:1116->192.31.7.130:80

  Ethernet Header:
    Destination MAC Addr     = 00A0C5921311
    Source MAC Addr          = 0080C84CEA63
    Network Type             = 0x0800 (TCP/IP)

  IP Header:
    IP Version               = 4
    Header Length            = 20
    Type of Service          = 0x00 (0)
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
    Total Length              = 0x0030 (48)
    Idetification             = 0x330B (13067)
    Flags                     = 0x02
    Fragment Offset           = 0x00
    Time to Live              = 0x80 (128)
    Protocol                  = 0x06 (TCP)
    Header Checksum           = 0x3E71 (15985)
    Source IP                 = 0xC0A80102 (192.168.1.2)
    Destination IP            = 0xC01F0782 (192.31.7.130)

  TCP Header:
    Source Port               = 0x045C (1116)
    Destination Port          = 0x0050 (80)
    Sequence Number           = 0x00BD15A7 (12391847)
    Ack Number                = 0x00000000 (0)
    Header Length             = 28
    Flags                     = 0x02 (....S.)
    Window Size               = 0x2000 (8192)
    Checksum                  = 0xBEC3 (48835)
    Urgent Ptr                = 0x0000 (0)
    Options                   =
        0000: 02 04 05 B4 01 01 04 02

  RAW DATA:
  0000: 00 A0 C5 92 13 11 00 80-C8 4C EA 63 08 00 45 00  .........L.c..E.
  0010: 00 30 33 0B 40 00 80 06-3E 71 C0 A8 01 02 C0 1F  .03.@...>q......
  0020: 07 82 04 5C 00 50 00 BD-15 A7 00 00 00 00 70 02  ...\.P........p.
  0030: 20 00 BE C3 00 00 02 04-05 B4 01 01 04 02         ............
---<0001>---------------------------------------------------------------
LAN Frame: ENET0-XMIT   Size:  58/  58   Time: 12090.020 sec
Frame Type: TCP 192.31.7.130:80->192.168.1.2:1116


  Ethernet Header:
    Destination MAC Addr      = 0080C84CEA63
    Source MAC Addr           = 00A0C5921311
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
  Network Type              = 0x0800 (TCP/IP)

IP Header:
  IP Version                = 4
  Header Length             = 20
  Type of Service           = 0x00 (0)
  Total Length              = 0x002C (44)
  Idetification             = 0x57F3 (22515)
  Flags                     = 0x02
  Fragment Offset           = 0x00
  Time to Live              = 0xED (237)
  Protocol                 = 0x06 (TCP)
  Header Checksum           = 0xAC8C (44172)
  Source IP                 = 0xC01F0782 (192.31.7.130)
  Destination IP            = 0xC0A80102 (192.168.1.2)

TCP Header:
  Source Port               = 0x0050 (80)
  Destination Port          = 0x045C (1116)
  Sequence Number           = 0x4AD1B57F (1255257471)
  Ack Number                = 0x00BD15A8 (12391848)
  Header Length             = 24
  Flags                     = 0x12 (.A..S.)
  Window Size               = 0xFAF0 (64240)
  Checksum                  = 0xF877 (63607)
  Urgent Ptr                = 0x0000 (0)
  Options                   =
      0000: 02 04 05 B4
```

```
RAW DATA:
0000: 00 80 C8 4C EA 63 00 A0-C5 92 13 11 08 00 45 00  ...L.c........E.
0010: 00 2C 57 F3 40 00 ED 06-AC 8C C0 1F 07 82 C0 A8  .,W.@...........
0020: 01 02 00 50 04 5C 4A D1-B5 7F 00 BD 15 A8 60 12  ...P.\J.......`.
0030: FA F0 F8 77 00 00 02 04-05 B4                    ...w......
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
---<0002>-----------------------------------------------------------------
LAN Frame: ENET0-RECV   Size:  60/  60   Time: 12090.210 sec
Frame Type: TCP 192.168.1.2:1116->192.31.7.130:80

  Ethernet Header:
    Destination MAC Addr     = 00A0C5921311
    Source MAC Addr          = 0080C84CEA63
    Network Type             = 0x0800 (TCP/IP)

  IP Header:
    IP Version               = 4
    Header Length            = 20
    Type of Service          = 0x00 (0)
    Total Length             = 0x0028 (40)
    Idetification            = 0x350B (13579)
    Flags                    = 0x02
    Fragment Offset          = 0x00
    Time to Live             = 0x80 (128)
    Protocol                 = 0x06 (TCP)
    Header Checksum          = 0x3C79 (15481)
    Source IP                = 0xC0A80102 (192.168.1.2)
    Destination IP           = 0xC01F0782 (192.31.7.130)


  TCP Header:
    Source Port              = 0x045C (1116)
    Destination Port         = 0x0050 (80)
    Sequence Number          = 0x00BD15A8 (12391848)
    Ack Number               = 0x4AD1B580 (1255257472)
    Header Length            = 20
    Flags                    = 0x10 (.A....)
    Window Size              = 0x2238 (8760)
    Checksum                 = 0xE8ED (59629)
    Urgent Ptr               = 0x0000 (0)
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
TCP Data: (Length=6, Captured=6)
  0000: 20 20 20 20 20 20

RAW DATA:
0000: 00 A0 C5 92 13 11 00 80-C8 4C EA 63 08 00 45 00  .........L.c..E.
0010: 00 28 35 0B 40 00 80 06-3C 79 C0 A8 01 02 C0 1F  .(5.@...<y......
0020: 07 82 04 5C 00 50 00 BD-15 A8 4A D1 B5 80 50 10  ...\.P....J...P.
0030: 22 38 E8 ED 00 00 20 20-20 20 20 20              "8....
```

2. Trace WAN packet

1.1 Disable to capture the LAN packet by entering: **sys trcp channel enet0 none**
1.2 Enable to capture the WAN packet by entering: **sys trcp channel enet1 bothway**
1.3 Enable the trace log by entering: **sys trcp sw on** & **sys trcl sw on**
1.4 Display the brief trace online by entering: **sys trcd brief**
or
1.5 Display the detailed trace online by entering: **sys trcd parse**

Example:

```
Prestige> sys trcp channel enet0 none
Prestige> sys trcp channel enet1 bothway
Prestige> sys trcp sw on
Prestige> sys trcl sw on
Prestige> sys trcd brief
0     12367.680 ENET1-R[0070] UDP 202.132.155.95:520->202.132.155.255:520
1     12370.980 ENET1-T[0062] TCP 202.132.155.97:10261->192.31.7.130:80
2     12373.940 ENET1-T[0062] TCP 202.132.155.97:10261->192.31.7.130:80
3     12374.930 ENET1-R[0064] TCP 192.31.7.130:80->202.132.155.97:10261
4     12374.940 ENET1-T[0054] TCP 202.132.155.97:10261->192.31.7.130:80
5     12374.940 ENET1-T[0438] TCP 202.132.155.97:10261->192.31.7.130:80
6     12375.320 ENET1-R[0064] TCP 192.31.7.130:80->202.132.155.97:10261
7     12375.360 ENET1-R[0090] UDP 202.132.155.95:520->202.132.155.255:520
Prestige> sys trcd parse
---<0000>----------------------------------------------------------------
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
LAN Frame: ENET1-RECV   Size:1181/  96   Time: 12387.260 sec
Frame Type: TCP 192.31.7.130:80->202.132.155.97:10270

  Ethernet Header:
    Destination MAC Addr      = 00A0C5921312
    Source MAC Addr           = 00A0C5012345
    Network Type              = 0x0800 (TCP/IP)

  IP Header:
    IP Version                = 4
    Header Length             = 20
    Type of Service           = 0x00 (0)
    Total Length              = 0x048B (1163)
    Idetification             = 0xB139 (45369)
    Flags                     = 0x02
    Fragment Offset           = 0x00
    Time to Live              = 0xEE (238)
    Protocol                  = 0x06 (TCP)
    Header Checksum           = 0xA9AB (43435)
    Source IP                 = 0xC01F0782 (192.31.7.130)
    Destination IP            = 0xCA849B61 (202.132.155.97)

  TCP Header:
    Source Port               = 0x0050 (80)
    Destination Port          = 0x281E (10270)
    Sequence Number           = 0xD3E95985 (3555285381)
    Ack Number                = 0x00C18F63 (12685155)
    Header Length             = 20
    Flags                     = 0x19 (.AP..F)
    Window Size               = 0xFAF0 (64240)
    Checksum                  = 0x3735 (14133)
    Urgent Ptr                = 0x0000 (0)

  TCP Data: (Length=1127, Captured=42)
  0000: DF 33 AF 62 58 37 52 3D-79 99 A5 3C 2B 59 E2 78  .3.bX7R=y..<+Y.x
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
  0010: A7 98 8F 3F A9 09 E4 0F-26 14 9C 58 3E 95 3E E7  ...?....&..X>.>.
  0020: FC 2A 4C 2F FB BE 2F FE-EF D0                    .*L/../...

  RAW DATA:
  0000: 00 A0 C5 92 13 12 00 A0-C5 01 23 45 08 00 45 00  ..........#E..E.
  0010: 04 8B B1 39 40 00 EE 06-A9 AB C0 1F 07 82 CA 84  ...9@...........
  0020: 9B 61 00 50 28 1E D3 E9-59 85 00 C1 8F 63 50 19  .a.P(...Y....cP.
  0030: FA F0 37 35 00 00 DF 33-AF 62 58 37 52 3D 79 99  ..75...3.bX7R=y.
  0040: A5 3C 2B 59 E2 78 A7 98-8F 3F A9 09 E4 0F 26 14  .<+Y.x...?....&.
  0050: 9C 58 3E 95 3E E7 FC 2A-4C 2F FB BE 2F FE EF D0  .X>.>..*L/../...
---<0001>--------------------------------------------------------------------
LAN Frame: ENET1-XMIT   Size:  54/  54   Time: 12387.490 sec
Frame Type: TCP 202.132.155.97:10270->192.31.7.130:80

  Ethernet Header:
    Destination MAC Addr     = 00A0C5012345
    Source MAC Addr          = 00A0C5921312
    Network Type             = 0x0800 (TCP/IP)

  IP Header:
    IP Version               = 4
    Header Length            = 20
    Type of Service          = 0x00 (0)
    Total Length             = 0x0028 (40)
    Idetification            = 0x7A0C (31244)
    Flags                    = 0x02
    Fragment Offset          = 0x00
    Time to Live             = 0x7F (127)
    Protocol                 = 0x06 (TCP)
    Header Checksum          = 0x543C (21564)
    Source IP                = 0xCA849B61 (202.132.155.97)
    Destination IP           = 0xC01F0782 (192.31.7.130)


  TCP Header:
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
    Source Port             = 0x281E (10270)
    Destination Port        = 0x0050 (80)
    Sequence Number         = 0x00C18F63 (12685155)
    Ack Number              = 0xD3E95DE9 (3555286505)
    Header Length           = 20
    Flags                   = 0x10 (.A....)
    Window Size             = 0x1DD5 (7637)
    Checksum                = 0x7A12 (31250)
    Urgent Ptr              = 0x0000 (0)

  RAW DATA:
  0000: 00 A0 C5 01 23 45 00 A0-C5 92 13 12 08 00 45 00  ....#E........E.
  0010: 00 28 7A 0C 40 00 7F 06-54 3C CA 84 9B 61 C0 1F  .(z.@...T<...a..
  0020: 07 82 28 1E 00 50 00 C1-8F 63 D3 E9 5D E9 50 10  ..(..P...c..].P.
  0030: 1D D5 7A 12 00 00                                ..z...
---<0002>---------------------------------------------------------------
LAN Frame: ENET1-XMIT   Size:  54/  54   Time: 12387.490 sec
Frame Type: TCP 202.132.155.97:10270->192.31.7.130:80


  Ethernet Header:
    Destination MAC Addr    = 00A0C5012345
    Source MAC Addr         = 00A0C5921312
    Network Type            = 0x0800 (TCP/IP)


  IP Header:
    IP Version              = 4
    Header Length           = 20
    Type of Service         = 0x00 (0)
    Total Length            = 0x0028 (40)
    Idetification           = 0x7B0C (31500)
    Flags                   = 0x02
    Fragment Offset         = 0x00
    Time to Live            = 0x7F (127)
    Protocol                = 0x06 (TCP)
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
    Header Checksum          = 0x533C (21308)
    Source IP                = 0xCA849B61 (202.132.155.97)
    Destination IP           = 0xC01F0782 (192.31.7.130)

  TCP Header:
    Source Port              = 0x281E (10270)
    Destination Port         = 0x0050 (80)
    Sequence Number          = 0x00C18F63 (12685155)
    Ack Number               = 0xD3E95DE9 (3555286505)
    Header Length            = 20
    Flags                    = 0x11 (.A...F)
    Window Size              = 0x1DD5 (7637)
    Checksum                 = 0x7A11 (31249)
    Urgent Ptr               = 0x0000 (0)

  RAW DATA:
  0000: 00 A0 C5 01 23 45 00 A0-C5 92 13 12 08 00 45 00  ....#E........E.
  0010: 00 28 7B 0C 40 00 7F 06-53 3C CA 84 9B 61 C0 1F  .({.@...S<...a..
  0020: 07 82 28 1E 00 50 00 C1-8F 63 D3 E9 5D E9 50 11  ..(..P...c..].P.
  0030: 1D D5 7A 11 00 00                                ..z...
Prestige>
```

Offline Trace

1. Trace LAN packet
2. Trace WAN packet

---

1. Trace LAN packet

1.1 Disable to capture the WAN packet by entering: **sys trcp channel enet1 none**
1.2 Enable to capture the LAN packet by entering: **sys trcp channel enet0 bothway**
1.3 Enable the trace log by entering: **sys trcp sw on** & **sys trcl sw on**
1.4 Wait for packet passing through Prestige over LAN

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

1.5 Disable the trace log by entering: **sys trcp sw off** & **sys trcl sw off**

1.6 Display the trace briefly by entering: **sys trcp brief**

1.7 Display specific packets by using: **sys trcp parse <from_index> <to_index>**

Exmaple:

```
Prestige> sys trcp channel enet1 none
Prestige> sys trcp channel enet0 bothway
Prestige> sys trcp sw on
Prestige> sys trcl sw on
Prestige> sys trcp sw off
Prestige> sys trcl sw off
Prestige> sys trcp brief
   0    10855.790 ENET0-T[0141] TCP 192.31.7.130:80->192.168.1.2:1102
   1    10855.800 ENET0-R[0060] TCP 192.168.1.2:1102->192.31.7.130:80
   2    10855.810 ENET0-R[0062] TCP 192.168.1.2:1103->192.31.7.130:80
   3    10855.840 ENET0-R[0062] TCP 192.168.1.2:1104->192.31.7.130:80
   4    10856.020 ENET0-T[0054] TCP 192.31.7.130:80->192.168.1.2:1102
   5    10856.030 ENET0-T[0058] TCP 192.31.7.130:80->192.168.1.2:1103
   6    10856.040 ENET0-R[0060] TCP 192.168.1.2:1103->192.31.7.130:80
Prestige> sys trcp parse 5 5
---<0005>--------------------------------------------------------------
LAN Frame: ENET0-XMIT   Size:  58/  58   Time: 10856.030 sec
Frame Type: TCP 192.31.7.130:80->192.168.1.2:1103

  Ethernet Header:
    Destination MAC Addr     = 0080C84CEA63
    Source MAC Addr          = 00A0C5921311
    Network Type             = 0x0800 (TCP/IP)

  IP Header:
    IP Version               = 4
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
   Header Length            = 20
   Type of Service          = 0x00 (0)
   Total Length             = 0x002C (44)
   Idetification            = 0x7F02 (32514)
   Flags                    = 0x02
   Fragment Offset          = 0x00
   Time to Live             = 0xED (237)
   Protocol                 = 0x06 (TCP)
   Header Checksum          = 0x857D (34173)
   Source IP                = 0xC01F0782 (192.31.7.130)
   Destination IP           = 0xC0A80102 (192.168.1.2)

 TCP Header:
   Source Port              = 0x0050 (80)
   Destination Port         = 0x044F (1103)
   Sequence Number          = 0xD91B1826 (3642431526)
   Ack Number               = 0x00AA405F (11157599)
   Header Length            = 24
   Flags                    = 0x12 (.A..S.)
   Window Size              = 0xFAF0 (64240)
   Checksum                 = 0xDCEF (56559)
   Urgent Ptr               = 0x0000 (0)
   Options                  =
       0000: 02 04 05 B4


 RAW DATA:
 0000: 00 80 C8 4C EA 63 00 A0-C5 92 13 11 08 00 45 00  ...L.c........E.
 0010: 00 2C 7F 02 40 00 ED 06-85 7D C0 1F 07 82 C0 A8  .,..@....}......
 0020: 01 02 00 50 04 4F D9 1B-18 26 00 AA 40 5F 60 12  ...P.O...&..@_`.
 0030: FA F0 DC EF 00 00 02 04-05 B4                    ..........
Prestige>
```

2. Trace WAN packet

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

1.1 Disable to capture the LAN packet by entering: **sys trcp channel enet0 none**
1.2 Enable to capture the WAN packet by entering: **sys trcp channel enet1 bothway**
1.3 Enable the trace log by entering: **sys trcp sw on** & **sys trcl sw on**
1.4 Wait for packet passing through Prestige over WAN
1.5 Disable the trace log by entering: **sys trcp sw off** & **sys trcl sw off**
1.6 Display the trace briefly by entering: **sys trcp brief**
1.7 Display specific packets by using: **sys trcp parse <from_index> <to_index>**

Example:

```
Prestige> sys trcp channel enet0 none
Prestige> sys trcp channel enet1 bothway
Prestige> sys trcl sw on
Prestige> sys trcp sw on
Prestige> sys trcl sw off
Prestige> sys trcp sw off
Prestige> sys trcp brief
   0    12864.800 ENET1-T[0411] TCP 202.132.155.97:10278->204.217.0.2:80
   1    12864.890 ENET1-R[0247] TCP 204.217.0.2:80->202.132.155.97:10282
   2    12864.900 ENET1-T[0416] TCP 202.132.155.97:10282->204.217.0.2:80
   3    12865.120 ENET1-R[0247] TCP 204.217.0.2:80->202.132.155.97:10278
   4    12865.130 ENET1-T[0411] TCP 202.132.155.97:10278->204.217.0.2:80
   5    12865.220 ENET1-R[0247] TCP 204.217.0.2:80->202.132.155.97:10282
Prestige> sys trcp parse 3 4
---<0003>--------------------------------------------------------------
LAN Frame: ENET1-RECV   Size: 247/  96   Time: 12865.120 sec
Frame Type: TCP 204.217.0.2:80->202.132.155.97:10278

  Ethernet Header:
    Destination MAC Addr     = 00A0C5921312
    Source MAC Addr          = 00A0C5591284
    Network Type             = 0x0800 (TCP/IP)

  IP Header:
    IP Version               = 4
    Header Length            = 20
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
  Type of Service          = 0x00 (0)
  Total Length             = 0x00E5 (229)
  Idetification            = 0xE93B (59707)
  Flags                    = 0x02
  Fragment Offset          = 0x00
  Time to Live             = 0xF0 (240)
  Protocol                 = 0x06 (TCP)
  Header Checksum          = 0x6E15 (28181)
  Source IP                = 0xCCD90002 (204.217.0.2)
  Destination IP           = 0xCA849B61 (202.132.155.97)

TCP Header:
  Source Port              = 0x0050 (80)
  Destination Port         = 0x2826 (10278)
  Sequence Number          = 0x4D713D8A (1299266954)
  Ack Number               = 0x00C8C015 (13156373)
  Header Length            = 20
  Flags                    = 0x18 (.AP...)
  Window Size              = 0x2238 (8760)
  Checksum                 = 0xAB57 (43863)
  Urgent Ptr               = 0x0000 (0)
```

```
TCP Data: (Length=193, Captured=42)
0000: 48 54 54 50 2F 31 2E 31-20 33 30 34 20 4E 6F 74  HTTP/1.1 304 Not
0010: 20 4D 6F 64 69 66 69 65-64 0D 0A 44 61 74 65 3A   Modified..Date:
0020: 20 57 65 64 2C 20 30 37-20 4A                     Wed, 07 J
```

```
RAW DATA:
0000: 00 A0 C5 92 13 12 00 A0-C5 59 12 84 08 00 45 00  .........Y....E.
0010: 00 E5 E9 3B 40 00 F0 06-6E 15 CC D9 00 02 CA 84  ...;@...n.......
0020: 9B 61 00 50 28 26 4D 71-3D 8A 00 C8 C0 15 50 18  .a.P(&Mq=.....P.
0030: 22 38 AB 57 00 00 48 54-54 50 2F 31 2E 31 20 33  "8.W..HTTP/1.1 3
0040: 30 34 20 4E 6F 74 20 4D-6F 64 69 66 69 65 64 0D  04 Not Modified.
0050: 0A 44 61 74 65 3A 20 57-65 64 2C 20 30 37 20 4A  .Date: Wed, 07 J
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
---<0004>-----------------------------------------------------------------
LAN Frame: ENET1-XMIT   Size: 411/  96   Time: 12865.130 sec
Frame Type: TCP 202.132.155.97:10278->204.217.0.2:80

  Ethernet Header:
    Destination MAC Addr     = 00A0C5591284
    Source MAC Addr          = 00A0C5921312
    Network Type             = 0x0800 (TCP/IP)

  IP Header:
    IP Version               = 4
    Header Length            = 20
    Type of Service          = 0x00 (0)
    Total Length             = 0x018D (397)
    Idetification            = 0xF20C (61964)
    Flags                    = 0x02
    Fragment Offset          = 0x00
    Time to Live             = 0x7F (127)
    Protocol                 = 0x06 (TCP)
    Header Checksum          = 0xD59C (54684)
    Source IP                = 0xCA849B61 (202.132.155.97)
    Destination IP           = 0xCCD90002 (204.217.0.2)


  TCP Header:
    Source Port              = 0x2826 (10278)
    Destination Port         = 0x0050 (80)
    Sequence Number          = 0x00C8C015 (13156373)
    Ack Number               = 0x4D713E47 (1299267143)
    Header Length            = 20
    Flags                    = 0x18 (.AP...)
    Window Size              = 0x1E87 (7815)
    Checksum                 = 0x4374 (17268)
    Urgent Ptr               = 0x0000 (0)

  TCP Data: (Length=357, Captured=42)
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
  0000: 47 45 54 20 2F 70 69 63-74 75 72 65 73 2F 6D 61  GET /pictures/ma
  0010: 67 61 7A 69 6E 65 5F 6C-6F 67 6F 2F 62 65 73 74  gazine_logo/best
  0020: 6F 66 74 69 6D 65 73 2E-67 69                    oftimes.gi

  RAW DATA:
  0000: 00 A0 C5 59 12 84 00 A0-C5 92 13 12 08 00 45 00  ...Y..........E.
  0010: 01 8D F2 0C 40 00 7F 06-D5 9C CA 84 9B 61 CC D9  ....@........a..
  0020: 00 02 28 26 00 50 00 C8-C0 15 4D 71 3E 47 50 18  ..(&.P....Mq>GP.
  0030: 1E 87 43 74 00 00 47 45-54 20 2F 70 69 63 74 75  ..Ct..GET /pictu
  0040: 72 65 73 2F 6D 61 67 61-7A 69 6E 65 5F 6C 6F 67  res/magazine_log
  0050: 6F 2F 62 65 73 74 6F 66-74 69 6D 65 73 2E 67 69  o/bestoftimes.gi
Prestige>
```

Debug PPPoE Connection

Debug PPPoE Connection

The ZyXEL device supports traces when there is problem to connect your ISP using PPPoE protocol. Please follow the procedure below to collect the trace for our troubleshooting.

1. Remove the LAN cable attached on the Prestige
2. Enter SMT using console port
3. Enter Menu 24.8-CI command mode
4. Type the following commands:
   - sys trcp sw on (turn on packet trace)
   - sys errctl 3 (save crash information and make system enter debug mode after the crash)
   - poe debug 1 (turn on pppoe debug)
   - dev dial 1 (dial remote node 1)
5. After all, if the Prestige crashes and you can do nothing, please send the above log back to us.
6. If the Prestige crashes and you are able to enter commands, please type 'atds' in debug mode to dump the log and send the log to us.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

7. If the Prestige does not crash but just can not dial out, please capture the following further log and send us the log.
    - sys trcp sw off (turn off packet trace)
    - sys log disp i (capture system error log)
    - sys trcp parse (parse the trace in detail)

Example- A trace with system crashes

```
ras> sys trcp sw on
ras> sys errctl 3
ras> poe debug 1
ras> dev dial 1
Start dialing for node <GPMI>...
poeNetCmdExe: chann poe0 event x420
poeChannDial: start session, peer<GPMI>
bdcastInit: pch poe0
poePut1SrvcName: '' len 0
host-uniq 31303030 len 4
putPoeHdr: ver 1 type 1 code x09 sess-id 0 len 12(x000C)
bdcastSendInit: l1.pktTx() failed, pch poe0 ch enet0
poePut1SrvcName: '' len 0
host-uniq 31303030 len 4
putPoeHdr: ver 1 type 1 code x09 sess-id 0 len 12(x000C)
### Hit any key to continue.###
$$$ DIALING dev=6 ch=0.........
poeI/C: ver 1 type 1 code x07 sessId x0000 len 274(x0112)
poeCtrlI/C: pkt len 274
poeGetTags()
service-name
service-name telstra
service-name bpa
service-name iprimus
service-name pacificinternet
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
service-name integrationisp
service-name bpa-dev
service-name bpa-sif
service-name telstrarna
service-name gpmsystems
service-name cmux
service-name launceston-broadband
service-name vivanet
service-name n1234567k00
service-name bigpond
service-name n7061992k
service-name n3068223k
service-name n2155202k
service-name n7061995k
AC-name vet1-exhibition-bsn-1
host-uniq 31303030 len 4
PADO recv'd, chann enet1
procPADO: for poe chann poe0
Chann poe0 sending request
poePut1SrvcName: '' len 0
host-uniq 31303030 len 4
putPoeHdr: ver 1 type 1 code x19 sess-id 0 len 12(x000C)
Undefined Address : 0xE3F045C4
Undefined Data : 0x56FF54FF
    r0= 0xE3F045C4    r1= 0x0001FFC0    r2= 0x000000E5    r3= 0x56FF54FF
    r4= 0xE3F045C4    r5= 0xE5BDBFEC    r6= 0x0001C468    r7= 0x60000093
    r8= 0x00000000    r9= 0xE3550000     r10=0xE3550000    fp= 0x00000000
    r12=0x56FF54FF    sp= 0x0001EDBC    lr= 0x00004F64    pc= 0x00013954
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
e5bdbfe0: e2 8f 00 06 e5 d5 20 06 e5 d5 20 0a e5 d5 20 0e ...b...f...j...n
e5bdbff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc000: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc010: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc020: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc030: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc040: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
e5bdc050: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc060: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc070: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc080: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc090: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc0a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc0b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc0c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc0d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
e5bdc0e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 ed 2b ...b...f...j...n
Bootbase Version: V1.06 | 11/05/2004 19:29:47
RAM: Size = 8192 Kbytes
DRAM POST: Testing:  8192K
OK
FLASH: Intel 16M

ZyNOS Version: V3.60(MM.0) | 12/31/2004 13:39:02
Enter Debug Mode
atgo
    (Compressed)
    Version: RAS P2302RLP1, start: bfc58030
    Length: 3DB3EC, Checksum: 9AA9
    Compressed Length: 12AC58, Checksum: DC06

Copyright (c) 1994 - 2005 ZyXEL Communications Corp.
initialize ch =0, ethernet address: 00:A0:C5:CB:A8:16
initialize ch =1, ethernet address: 00:A0:C5:CB:A8:17
VC5402 Init...OK
Press ENTER to continue...

               Enter Password : XXXX
```

LAN/WAN Packet Trace

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

The ZyXEL device packet trace records and analyzes packets running on LAN and WAN interfaces. It is designed for users with technical backgrounds who are interested in the details of the packet flow on LAN or WAN end of Prestige. It is also very helpful for diagnostics if you have compatibility problems with your ISP or if you want to know the details of a packet for configuring a filter rule.

The format of the display is as following:

Packet:

```
0    11880.160 ENET0-R[0062] TCP 192.168.1.2:1108->192.31.7.130:80
```

[index] [timer/second][channel-receive/transmit][length] [protocol] [sourceIP/port] [destIP/port]

There are two ways to dump the trace:

1. **Online Trace--display the trace real time on screen**
2. **Offline Trace--capture the trace first and display later**

The details for capturing the trace in SMT menu 24.8 are as follows.

Online Trace

1. Trace LAN packet
2. Trace WAN packet

---

1. Trace LAN packet

1.1 Disable to capture the WAN packet by entering: `sys trcp channel mpoa00 none`
1.2 Enable to capture the LAN packet by entering: `sys trcp channel enet0 bothway`
1.3 Enable the trace log by entering: `sys trcp sw on` & **`sys trcl sw on`**
1.4 Display the brief trace online by entering: `sys trcd brief`
or
1.5 Display the detailed trace online by entering: `sys trcd parse`

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

Example:

```
ras> sys trcp channel mpoa00 none
ras> sys trcp channel enet0 bothway
ras> sys trcp sw on
ras> sys trcl sw on
ras> sys trcd brief
   0    11880.160 ENET0-R[0062] TCP 192.168.1.2:1108->192.31.7.130:80
   1    11883.100 ENET0-R[0062] TCP 192.168.1.2:1108->192.31.7.130:80
   2    11883.330 ENET0-T[0058] TCP 192.31.7.130:80->192.168.1.2:1108
   3    11883.340 ENET0-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
   4    11883.340 ENET0-R[0339] TCP 192.168.1.2:1108->192.31.7.130:80
   5    11883.610 ENET0-T[0054] TCP 192.31.7.130:80->192.168.1.2:1108
   6    11883.620 ENET0-T[0102] TCP 192.31.7.130:80->192.168.1.2:1108
   7    11883.630 ENET0-T[0054] TCP 192.31.7.130:80->192.168.1.2:1108
   8    11883.630 ENET0-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
   9    11883.2602HW ENET0-R[0060] TCP 192.168.1.2:1108->192.31.7.130:80
  10    11883.2602HW ENET0-R[0062] TCP 192.168.1.2:1109->192.31.7.130:80
ras> sys trcd parse
---<0000>--------------------------------------------------------------------
LAN Frame: ENET0-RECV   Size:  62/  62   Time: 12089.790 sec
Frame Type: TCP 192.168.1.2:1116->192.31.7.130:80

  Ethernet Header:
    Destination MAC Addr     = 00A0C5921311
    Source MAC Addr          = 0080C84CEA63
    Network Type             = 0x0800 (TCP/IP)

  IP Header:
    IP Version               = 4
    Header Length            = 20
    Type of Service          = 0x00 (0)
    Total Length             = 0x0030 (48)
    Idetification            = 0x330B (13067)
    Flags                    = 0x02
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
    Fragment Offset          = 0x00
    Time to Live             = 0x80 (128)
    Protocol                 = 0x06 (TCP)
    Header Checksum          = 0x3E71 (15985)
    Source IP                = 0xC0A80102 (192.168.1.2)
    Destination IP           = 0xC01F0782 (192.31.7.130)

  TCP Header:
    Source Port              = 0x045C (1116)
    Destination Port         = 0x0050 (80)
    Sequence Number          = 0x00BD15A7 (12391847)
    Ack Number               = 0x00000000 (0)
    Header Length            = 28
    Flags                    = 0x02 (....S.)
    Window Size              = 0x2004 (8192)
    Checksum                 = 0xBEC3 (48835)
    Urgent Ptr               = 0x0000 (0)
    Options                  =
        0000: 02 04 05 B4 01 01 04 02

  RAW DATA:
  0000: 00 A0 C5 92 13 11 00 80-C8 4C EA 63 08 00 45 00  .........L.c..E.
  0010: 00 30 33 0B 40 00 80 06-3E 71 C0 A8 01 02 C0 1F  .03.@...>q......
  0020: 07 82 04 5C 00 50 00 BD-15 A7 00 00 00 00 70 02  ...\.P........p.
  0030: 20 00 BE C3 00 00 02 04-05 B4 01 01 04 02         ............
---<0001>---------------------------------------------------------------
LAN Frame: ENET0-XMIT   Size:  58/  58   Time: 12090.020 sec
Frame Type: TCP 192.31.7.130:80->192.168.1.2:1116

  Ethernet Header:
    Destination MAC Addr     = 0080C84CEA63
    Source MAC Addr          = 00A0C5921311
    Network Type             = 0x0800 (TCP/IP)

  IP Header:
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
   IP Version               = 4
   Header Length            = 20
   Type of Service          = 0x00 (0)
   Total Length             = 0x002C (44)
   Idetification            = 0x57F3 (22515)
   Flags                    = 0x02
   Fragment Offset          = 0x00
   Time to Live             = 0xED (237)
   Protocol                = 0x06 (TCP)
   Header Checksum          = 0xAC8C (44172)
   Source IP                = 0xC01F0782 (192.31.7.130)
   Destination IP           = 0xC0A80102 (192.168.1.2)

 TCP Header:
   Source Port              = 0x0050 (80)
   Destination Port         = 0x045C (1116)
   Sequence Number          = 0x4AD1B57F (1255257471)
   Ack Number               = 0x00BD15A8 (12391848)
   Header Length            = 24
   Flags                    = 0x12 (.A..S.)
   Window Size              = 0xFAF0 (2602HW40)
   Checksum                 = 0xF877 (63607)
   Urgent Ptr               = 0x0000 (0)
   Options                  =
       0000: 02 04 05 B4

 RAW DATA:
 0000: 00 80 C8 4C EA 63 00 A0-C5 92 13 11 08 00 45 00  ...L.c........E.
 0010: 00 2C 57 F3 40 00 ED 06-AC 8C C0 1F 07 82 C0 A8  .,W.@...........
 0020: 01 02 00 50 04 5C 4A D1-B5 7F 00 BD 15 A8 60 12  ...P.\J.......`.
 0030: FA F0 F8 77 00 00 02 04-05 B4                    ...w......
---<0002>---------------------------------------------------------------
LAN Frame: ENET0-RECV   Size:  60/  60   Time: 12090.210 sec
Frame Type: TCP 192.168.1.2:1116->192.31.7.130:80
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
Ethernet Header:
  Destination MAC Addr     = 00A0C5921311
  Source MAC Addr          = 0080C84CEA63
  Network Type             = 0x0800 (TCP/IP)

IP Header:
  IP Version               = 4
  Header Length            = 20
  Type of Service          = 0x00 (0)
  Total Length             = 0x0028 (40)
  Idetification            = 0x350B (13579)
  Flags                    = 0x02
  Fragment Offset          = 0x00
  Time to Live             = 0x80 (128)
  Protocol                 = 0x06 (TCP)
  Header Checksum          = 0x3C79 (15481)
  Source IP                = 0xC0A80102 (192.168.1.2)
  Destination IP           = 0xC01F0782 (192.31.7.130)

TCP Header:
  Source Port              = 0x045C (1116)
  Destination Port         = 0x0050 (80)
  Sequence Number          = 0x00BD15A8 (12391848)
  Ack Number               = 0x4AD1B580 (1255257472)
  Header Length            = 20
  Flags                    = 0x10 (.A....)
  Window Size              = 0x2238 (8760)
  Checksum                 = 0xE8ED (59629)
  Urgent Ptr               = 0x0000 (0)

TCP Data: (Length=6, Captured=6)
  0000: 20 20 20 20 20 20

RAW DATA:
0000: 00 A0 C5 92 13 11 00 80-C8 4C EA 63 08 00 45 00  .........L.c..E.
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
0010: 00 28 35 0B 40 00 80 06-3C 79 C0 A8 01 02 C0 1F  .(5.@...<y......
0020: 07 82 04 5C 00 50 00 BD-15 A8 4A D1 B5 80 50 10  ...\.P....J...P.
0030: 22 38 E8 ED 00 00 20 20-20 20 20 20              "8....
```

2. Trace WAN packet

1.1 Disable the capture of the LAN packet by entering: **sys trcp channel enet0 none**
1.2 Enable to capture the WAN packet by entering: **sys trcp channel mpoa00 bothway**
1.3 Enable the trace log by entering: **sys trcp sw on** & **sys trcl sw on**
1.4 Display the brief trace online by entering: **sys trcd brief**
or
1.5 Display the detailed trace online by entering: **sys trcd parse**

Example:

```
ras> sys trcp channel enet0 none
ras> sys trcp channel mpoa00 bothway
ras> sys trcp sw on
ras> sys trcl sw on
ras> sys trcd brief
0    12367.680 MPOA00-R[0070] UDP 202.132.155.95:520->202.132.155.255:520
1    12370.980 MPOA00-T[0062] TCP 202.132.155.97:10261->192.31.7.130:80
ras> sys trcd parse
---<0000>--------------------------------------------------------------
LAN Frame: MPOA00-RECV   Size:1181/  96   Time: 12387.260 sec
Frame Type: TCP 192.31.7.130:80->202.132.155.97:10270

  Ethernet Header:
    Destination MAC Addr     = 00A0C5921312
    Source MAC Addr          = 00A0C5012345
    Network Type             = 0x0800 (TCP/IP)

  IP Header:
    IP Version               = 4
    Header Length            = 20
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

```
  Type of Service          = 0x00 (0)
  Total Length             = 0x048B (1163)
  Idetification            = 0xB139 (45369)
  Flags                    = 0x02
  Fragment Offset          = 0x00
  Time to Live             = 0xEE (238)
  Protocol                 = 0x06 (TCP)
  Header Checksum          = 0xA9AB (43435)
  Source IP                = 0xC01F0782 (192.31.7.130)
  Destination IP           = 0xCA849B61 (202.132.155.97)

TCP Header:
  Source Port              = 0x0050 (80)
  Destination Port         = 0x281E (10270)
  Sequence Number          = 0xD3E95985 (3555285381)
  Ack Number               = 0x00C18F63 (12685155)
  Header Length            = 20
  Flags                    = 0x19 (.AP..F)
  Window Size              = 0xFAF0 (2602HW40)
  Checksum                 = 0x3735 (14133)
  Urgent Ptr               = 0x0000 (0)

TCP Data: (Length=1127, Captured=42)
0000: DF 33 AF 62 58 37 52 3D-79 99 A5 3C 2B 59 E2 78  .3.bX7R=y..<+Y.x
0010: A7 98 8F 3F A9 09 E4 0F-26 14 9C 58 3E 95 3E E7  ...?....&..X>.>.
0020: FC 2A 4C 2F FB BE 2F FE-EF D0                    .*L/../...
```

```
RAW DATA:
0000: 00 A0 C5 92 13 12 00 A0-C5 01 23 45 08 00 45 00  ..........#E..E.
0010: 04 8B B1 39 40 00 EE 06-A9 AB C0 1F 07 82 CA 84  ...9@...........
0020: 9B 61 00 50 28 1E D3 E9-59 85 00 C1 8F 63 50 19  .a.P(...Y....cP.
0030: FA F0 37 35 00 00 DF 33-AF 62 58 37 52 3D 79 99  ..75...3.bX7R=y.
0040: A5 3C 2B 59 E2 78 A7 98-8F 3F A9 09 E4 0F 26 14  .<+Y.x...?....&.
0050: 9C 58 3E 95 3E E7 FC 2A-4C 2F FB BE 2F FE EF D0  .X>.>..*L/../...
```

All contents Copyright (c) 2007 ZyXEL Communications Corporation.

Offline Trace

1. Trace LAN packet
2. Trace WAN packet

---

1. Trace LAN packet

1.1 Disable the capture of the WAN packet by entering: `sys trcp channel mpoa00 none`
1.2 Enable the capture of the LAN packet by entering: `sys trcp channel enet0 bothway`
1.3 Enable the trace log by entering: `sys trcp sw on` & **`sys trcl sw on`**
1.4 Wait for packet passing through the Prestige over LAN
1.5 Disable the trace log by entering: `sys trcp sw off` & **`sys trcl sw off`**
1.6 Display the trace briefly by entering: `sys trcp brief`
1.7 Display specific packets by using: `sys trcp parse <from_index> <to_index>`

2. Trace WAN packet

1.1 Disable the capture of the LAN packet by entering: `sys trcp channel enet0 none`
1.2 Enable the capture of the WAN packet by entering: `sys trcp channel mpoa00 bothway`
1.3 Enable the trace log by entering: `sys trcp sw on` & **`sys trcl sw on`**
1.4 Wait for packet passing through the Prestige over WAN
1.5 Disable the trace log by entering: `sys trcp sw off` & **`sys trcl sw off`**
1.6 Display the trace briefly by entering: `sys trcp brief`
1.7 Display specific packets by using: `sys trcp parse <from_index> <to_index>`

CLI Command List

The latest CI command list is available in release notes of every ZyXEL firmware release. Please go to ZyXEL public WEB site http://www.zyxel.com/support/download.php to download firmware package (*.zip), you should unzip the package to get the release note in PDF format.

All contents Copyright (c) 2007 ZyXEL Communications Corporation.